НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
"КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"

ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ
НДІ ТЕЛЕКОМУНІКАЦІЙ

Десята міжнародна науково-технічна конференція "ПРОБЛЕМИ ТЕЛЕКОМУНІКАЦІЙ"

і

Восьма Міжнародна науково-технічна конференція студентів та аспірантів «ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА СИСТЕМ»

Присвячено Дню науки та Всесвітньому Дню телекомунікацій

19–22 квітня 2016 року

Матеріали конференції

м. Київ

NATIONAL TECHNICAL UNIVERSITY OF UKRAINE
“KYIV POLYTECHNIC INSTITUTE”

INSTITUTE OF TELECOMMUNICATION SYSTEMS
RESEARCH INSTITUTE OF TELECOMMUNICATIONS

Tenth International Scientific Conference
"MODERN CHALLENGES IN TELECOMMUNICATIONS"

and

Eighth International Scientific Conference of undergraduate and graduate students "PROSPECTS FOR DEVELOPMENT OF INFORMATION-TELECOMMUNICATION TECHNOLOGIES AND SYSTEMS"

Dedicated to the Science Day and the International Day of Telecommunication

April 19-22, 2016

Conference materials

Kyiv

X Міжнародна науково-технічна конференція "Проблеми телекомунікацій" ПТ-2016: Збірник матеріалів конференції. К.: НТУУ "КПІ", 2016. – 582 с.

VIII Міжнародна науково-технічна конференція студентів та аспірантів «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем» ПРІТС 2016: Збірник тез конференції. К.: НТУУ "КПІ", 2016.

Збірник містить матеріали пленарних і секційних доповідей, представлених на Десятій міжнародній науково-технічній конференції "Проблеми телекомунікацій" (ПТ 2016) та Восьмій Міжнародній науково-технічній конференції студентів та аспірантів «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем» (ПРІТС 2016), які проводяться 19–22 квітня 2016 р. в м. Києві.

Робочими мовами конференцій є українська, російська та англійська.

У збірник включені матеріали конференції за такими секціями:

1. Передавання інформації в телекомунікаційних системах.
2. Кабельні та оптоволоконні системи і технології.
3. Технології транспортних телекомунікаційних систем та мережні технології.
4. Безпроводові телекомунікаційні системи та технології.
5. Інформаційні технології в телекомунікаціях.
6. Сенсорні мережі та прикладні аспекти застосування телекомунікаційних технологій.
7. Засоби та пристрої телекомунікацій.
8. Підготовка кадрів телекомунікаційного профілю, історія розвитку телекомунікацій.
9. Семінар: Modern information and telecommunication trends.

Вчений секретар конференції
БУНІН С.Г., д.т.н., проф. ІТС НТУУ "КПІ".
E-mail: sgbunin@ukr.net

Секретар оргкомітету конференції
Іванова Т.Л.
р. тел/факс. (044)204-98-21.
E-mail: ivanova@its.kpi.ua

Співголови конференції "Проблеми телекомунікацій":

БАРАНОВ О.А. – Член Консультативної ради з питань інформатизації при Верховній Раді України, д.т.н., професор.

ІЛЬЧЕНКО М.Ю. – проректор з наукової роботи Національного технічного університету України "Київський політехнічний інститут", академік НАНУ, д.т.н., професор.

Організатори конференції:

Національний технічний університет України «КПІ», ІТС, НДІТ;
Міжнародний науково-технічний журнал «TELECOMMUNICATION SCIENCES» ISSN: 2312-4121.

Спонсори конференції:

Організації та підприємства, які приймають участь у науковій праці й працевлаштуванні випускників ІТС, а також всі бажаючі.

Координатор Програмного комітету:

КРАВЧУК С.О. - д.т.н., проф., НТУУ «КПІ», Київ,
e-mail: sakravchuk@ukr.net

Члени Програмного комітету "Проблеми телекомунікацій":

Богуш В. М. - к.т.н., доц., НАУ, м. Київ
Бунін С.Г. – д.т.н., проф. ІТС НТУУ «КПІ», м. Київ
Глоба Л.С. – д.т.н., проф., зав. каф. ІТС НТУУ «КПІ»,м. Київ
Жук С.Я. – д.т.н., проф., РТФ НТУУ «КПІ», м. Київ
Зависляк І.В. – д.ф.м.н., проф., КНУ ім. Т. Шевченко, м. Київ
Капштик С.В. – к.т.н., доц., НТУУ «КПІ», м. Київ
Каток В.Б. – к.т.н., проф., Укртелеком, м. Київ
Козелков С.В. – д.т.н., проф. ДУТ, м. Київ
Лемешко О.В. – д.т.н., проф., ХНУР, м. Харків
Лисенко О.І. – д.т.н., проф., ІТС НТУУ «КПІ», м. Київ

Ліпатов А.О. – к.т.н., проф., ІТС НТУУ «КПІ», м. Київ
Максимов В.В. – к.т.н., доц., ІТС НТУУ «КПІ» м. Київ
Мошинська А.В. – к.т.н., доц., ІТС НТУУ «КПІ» м. Київ
Наритник Т.М. – к.т.н., проф., ІТС НТУУ «КПІ», м. Київ
Назаренко О.І. – факультет лінгвістики НТУУ „КПІ”, м. Київ;
Поплавко Ю. М. – д.ф.м.н., проф., НТУУ «КПІ», м. Київ
Поповський В.В. – д.т.н., проф. ХНУРЕ, м. Харків
Романов О.І. – д.т.н., проф. ІТС НТУУ «КПІ», м. Київ
Романюк В.А. – д.т.н., проф. ДУТ, м. Київ
Скулиш М.А. – к.т.н., доц., ІТС НТУУ «КПІ», м. Київ
Стрижак О.Є. – к.т.н., НЦ «Мала АНУ», м. Київ
Міночкін Д.А. – к.т.н., ст..викл., ІТС НТУУ «КПІ», м. Київ
Толюпа С.В. – д.т.н., проф., КГУ, м. Київ
Трубін О.О. – д.т.н.,проф., ІТС НТУУ «КПІ», м. Київ
Уривський Л.О. – д.т.н., проф., ІТС НТУУ «КПІ», м. Київ
Чечельницький В.Я. – д.т.н., проф., ОНПУ, м. Одеса
Чумаченко С.М. – д.т.н., с.н.с., УНДІЦЗ, м. Київ
Шелковніков Б.М. – к.т.н., доц., ІТС НТУУ «КПІ» м. Київ
Явіся В.С. – к.т.н., доц., НТУУ «КПІ», м. Київ
Якорнов Є.А. – к.т.н., проф., заст. директора ІТС НТУУ «КПІ», м. Київ

Технічний комітет:

1. Слюсар В.С. – транспорт, поселення, р.т. 204-98-21.
2. Дуля Ю.А. – головний бухгалтер НДІ ТК, р.т. 236-95-04.
3. Березовська О.В. – реєстрація, забезпечення документообігу, р.т. 204-98-21.
4. Мікляєв О.В. – технічне обслуговування електронної техніки, р.т. 204-98-21.
5. Мазанка Р.М. – оформлення конференції на сайті ІТС, р.т. 204-98-91.

Адреса для листування, телефони:

03056, г. Київ, провулок Індустріальний, 2, корпус 30, секретарю оргкомітету конференції «ПТ» Івановій Т.Л., р.тел/факс. (044)204-98-21.

Адреса проведення конференції:

03056, г. Київ, провулок Індустріальний, 2, корпус № 30 НТУУ «КПІ», 4 поверх.

ЗМІСТ

Пленарні доповіді

Доповідачі:

Ильченко М.Е., Живков А.П. *Инверсия мод колебаний в ячейках метаматериалов.* 20

Trubin A. A. *Scattering of electromagnetic waves on different dielectric resonator structures*.....24

Андрей Дудченко *Internet Of Things. Что это такое, перспективы и реализация* 27

Уривський Л.О., Осипчук С.О., Шмігель Б.О. *Особливості способів оцінки продуктивності мережі на основі 802.11ac* 28

Ільченко М.Ю., Кравчук С.О., Міночкін Д.А., Явіся В.С. *Спеціальність телекомунікації та радіотехніка: нові спеціалізації* 31

Лемешко О.В., Єременко О.С. *Особливості використання тензорного підходу для опису динаміки зміни стану мережі при забезпеченні якості обслуговування* 34

Климаш М.М., Бешлей М.І., Масюк А.Р. *Розробка та дослідження імітаційної моделі безпровідної гетерогенної мережі* 37

Станкевич С.А., Шкляр С.В., Подорван В.М., Лубський М.С. *Підвищення інформативності зображень дальнього інфрачервоного діапазону на основі субпіксельної обробки* 40

Романюк В.А. *Цільові функції управління повітряною радіомережею* 43

Орищук М.В., Романов О.І. *Методика розрахунку вимушеного Раманівського розсіювання в DWDM системі* 48

Лисенко О.І., Валуйський С.В. *Прикладні аспекти застосування безпроводових сенсорних мереж і БПЛА* 51

Секція 1. Передавання інформації в телекомунікаційних системах

Співголови: д.т.н., проф. Уривський Л.О., к.т.н., доц. Максимов В.В., к.т.н., доц. Мошинська А.В.

Доповідачі:

Шевчук Б.М. Методи та алгоритми кодування і передачі моніторингових даних в інформаційно-ефективних радіомережах. 55

Пєшкін А.М., Уривський Л.О. Аналіз принципів формування та коригуючих можливостей каскадних кодів..... 58

Мошинская А.В., Георгин Д.А. Синтез методики оценки качества цифрового сигнала. 62

Прокушев А.Н., Ступак Г.В., Бойко В.В. Исследование качественных характеристик VOIP..... 65

Шостак Н.В. Характеристики оцінки якості стегосистем..... 68

Гайворонська Г.С., Брицький С.В. Дослідження доцільності використання методів теорії прийняття рішень при синтезі мереж доступу 71

Гайворонская Г.С., Казак Ю.С. Разработка модели синтеза сети доступа при использовании теории метапроцедур..... 74

Гайворонская Г.С., Рыбалов Б.А. Исследование возможности использования оптических процессоров для управления коммутацией оптических сигналов..... 77

Правило В.В. Розрахунок показників якості категорійного обслуговування заявок при абсолютному пріоритеті на інтелектуальній мережі зв'язку..... 80

Правило В.В. Синтез раціональної структури телекомунікаційної мережі за заданими показниками 83

Куляс А.А., Носков В.І. Оцінка пропускної спроможності SHDSL-системи передачі з використанням технології EFM..... 86

Максимов В.В., Литвин О.О. Класифікація протоколів MAC рівня для AD-HOC мереж..... 89

Дищук А.С. Аналіз функціонування складного об'єкту системи управління в телекомунікаціях 92

Осипчук И.С., Чекунов Н.В., Осипчук С.А. Исследование мультисервисной сети связи на основе стандарта 802.11N..... 95

Максимов В.В., Кулик М.В. Класифікація моделей переміщення вузлів у мережах MANET..... 98

1. **Гаттуров В.К., Цыпанов В.А.** Туннелирование и виртуальные частные сети на основе MPLS. 101

Шаповалов Р.С., Гаттуров В.К. Захист транспортних мереж від DDoS атак..... 104

Секція 2. Кабельні та оптоволоконні системи і технології

Секція 8. Підготовка кадрів телекомунікаційного профілю, історія розвитку телекомунікацій

Співголови: проф. Якорнов Є.А., к.т.н., проф. Каток В.Б., к.т.н., доц. Явіся В.С.

Доповідачі:

Кайдан М.В., Андрущак В.С. Оцінка параметру енергоефективності оптичних транспортних мереж на базі електрооптичних пристроїв 107

Харченко М.О., Каток В.Б. Оптична надійність волоконно-оптичних кабелів зв'язку в результаті старіння 110

Федюшина Д.М., Каток В.Б. мультисервісні мережі доступу на базі архітектури PON для котеджної забудови 113

Воронін Р.О., Каток В.Б. Застосування технології GPON у мультисервісних мережах доступу 116

Сапа Т.І. Побудова мережі FTTH на основі мікротрубчатої каналізації для районів індивідуального житла 119

Филинюк М.А., Лищинская Л.Б., Стахов В.П. Исследование помехоустойчивости моноиммитансного логического R-элемента «И» 122

Тимченко И.О., Сундучков К.С. Будущее спутникового интернета..... 125

Парфенюк В.Г. Досвід використання програмного комплексу LABVIEW у навчальному процесі та у наукових дослідженнях 128

Могильний С.Б. Технології «ІНТЕРНЕТУ РЕЧЕЙ» - підготовка фахівців актуально в часі 131

Рябенко М.С., Голь В.Д., Явіся В.С. Засіб підвищення ефективності навчання спеціалістів практичним навичкам при роботі з технічними пристроями 134

Секція 3. Технології транспортних телекомунікаційних систем та мережні технології

Співголови: д.т.н., проф. Романов О.І., д.т.н., проф. Лемешко О.В.

Доповідачі:

Безрук В.М., Чеботарёва Д.В., Скорик Ю.В. Многокритериальный выбор оптимальных средств телекоммуникаций 137

Червенець В.В., Бешлей М.І., Романчук В.І. Поліщук А.В. Модель віртуального маршрутизатора з статичною та динамічною реконфігурацією ресурсів 140

Горбачук В. М., Морозов О. О. До вимірювання системних ризиків мереж 143

Бирюков Н.Л., Триска Н.Р., Худынцев Н.Н. Оценка стабильности сигналов синхронизации в современных пакетных сетях 146

Толстова А.В., Голь В.Д., Правило В.В. Порівняльний аналіз асиметричних криптографічних методів 149

Пилипенко Б.В., Голь В.Д., Правило В.В. Аналіз протоколу otr шифрування для обміну миттєвими повідомленнями 152

Романов О.И., Верес Л.А., Явіся В.С. Анализ основных протоколов архитектуры IMS 155

Міночкін Д.А. Використання програмно-визначених мереж для модернізації IT-інфрастуктури мобільного зв'язку 158

Бірюков М.Л., Дяченко А.П. Перспективи використання технології PON в якості мережі синхронізації 161

Штепа В.О., Латуха А.В. Основні принципи управління мережевими ресурсами в архітектурі програмно-визначених мереж 164

Романов О. І., Москвитіна А. О. Модель процесу управління захистом від перенавантажень мереж передачі даних 167

Романов О.І., Гордашник Є.С. Аналіз і класифікація атак в мережах IP-телефонії на базі SOFTSWITCH CLASS V 170

Харлай Л.О. Методи селекції перевантажень та відмов мережних вузлів 173

Нестеренко М.М., Романов А.О. Аналіз методів захисту серверів від розподілених TCP SYN-FLOOD атак 176

Маньковский В.Б. Оценка производительности трафика в сети MPLS с использованием TRAFFIC ENGINEERING 179

Роговой В. П. Центры обработки данных на базе технологии SDN 182

Мишко М. С., Авдеенко Г.Л. Программная IP АТС: преимущества и недостатки 185

Галенко Е.В., Лисковский И.О. Проблемы обеспечения гарантированного предоставления сервисов в телекоммуникационной сети 188

Марціленко С.В., Глоба Л.С. Застосування прогамно-визначуваних мереж (SDN) в технології 5G 191

Секція 4. Безпроводові телекомунікаційні технології

Співголови: д.т.н., проф. Наритник Т.М., д.т.н., проф. Кравчук С.О.

Доповідачі:

Наритник Т.Н., Набока Б.Ю., Авдєєнко Г.Л. Дослідження передавання радіосигналу цифрового телебачення стандарту DVB-S з використанням радіоканалу терагерцового діапазону 194

Наритник Т.Н., Набока Б.Ю., Авдєєнко Г.Л. Дослідження передачі сигналів DVB-C по радіорелейній лінії терагерцового діапазону 198

Приступчук Ю.А., Половий О.М., Шелковников Б.М. Характеристика безспроводної системи для діапазону 240 ГГц..... 201

Авдєєнко Г.Л, Адамович О.М. Дослідження можливості передачі сигналу цифрового телебачення стандарту DVB-T2 по радіорелейній лінії методом комбінованої. 204

Гордеева Д.С., Курдеча В.В. Развертывание малых сот для энергоэффективной гетерогенной сотовой сети. 207

Цуканов О.Ф., Якорнов Е.А. Оценка дисперсии дальности до источника радиоизлучения по результатам измерения фазовых сдвигов для выбора максимального количества элементов антенной решетки. 210

Наритник Т.Н., Єрмаков А.В., Казіміренко В.Я., Сайко В.Г. Дослідження мережі широкосмугового абонентського доступу до інформаційних ресурсів в терагерцовому діапазоні..... 213

Лазарєв К. Д., Лісковський І. О. Продуктивність сервісів, що надаються мобільними операторами..... 216

Дудник А. В., Авдєєнко Г. Л. Аналіз існуючих технічних рішень та обґрунтування вибору радіомодулю для побудови приймача сигналів систем супутникової радіонавігації GPS та ГЛОНАСС. 218

Солянікова В.Ю., Дудник А.В., Авдєєнко Г.Л. Дослідження функціональних можливостей навігаційних приймачів сигналів GPS/GLONASS. 221

Гузовская М.В., Кайденко Н.Н. Канальная адаптация в системах широкополосного радиодоступа IEEE 802.16-2009 224

Єрохін В.Ф., Пелешок Є.В., Захарич О.В. Математична модель когерентної демодуляції взаємнозаважаючих цифрових сигналів з мінімальною частотною маніпуляцією..... 227

Примаченко В.І., Сторчак К.П., Макаренко А.О. Математичне моделювання безпроводових телекомунікаційних систем..... 230

Макаренко А.О., Гринкевич Г.О., Срочинська Г.С. Технічні особливості проектування багатоканальних систем для декількох користувачів..... 233

Сальник С.В., Сальник В.В., Лукіна К.В. Метод навчання бази знань підсистеми забезпечення безпеки мобільної радіомережі класу MANET на основі нечіткої логіки та апарату 236

Кувшинов О.В., Борознюк М.В., Рубцов І.Ю. Методика вибору робочих частот для систем радіозв'язку з псевдовипадковою перестройкою робочої частоти 239

Руденко Д.М. Оцінки ймовірності правильного виявлення сигналів з Райсовськими завмираннями 242

Пустовой Б. Л., Кунуп Т.В. Оценка эффективности управления интеллектуальными услугами..... 244

Гуськов П.О., Бак Р.І. Метод розміщення базових станцій в мережах мобільного зв'язку п'ятого покоління 247

Кайденко Н.Н., Кайденко В.Н. Программно-аппаратное моделирование телекоммуникационных процессов и систем В MATLAB с использованием SDR и SOC технологий..... 250

Кайденко В.М., Кайденко М.М., Крылач О.Ф., Роскошний Д.В. Организация взаимодействия между HPS и FPGA на базе SoC технологий при создании телекоммуникационных устройств. 254

Афанасьєва Л. О., Кравчук І.М., Кравчук С.О. Метод кооперативного рознесення. 257

Афанасьєва Л.О. Пропускна здатність каналів з кооперативною ретрансляцією..... 260

Афанасьєва Л.О., Кравчук І.М., Кравчук С.О. Модель багатостільникової мережі з MIMO – кооперацією 263

Довгань Б.М, Кравчук С.О. Процедури вертикальної передачі обслуговування для безпроводових мереж 4-го покоління..... 266

Кисельов В. О., Кравчук С. О. Зменшення впливу співканальних завад в безпроводових мережах з ретрансляцією. 269

Мєлєхова М.О., Кравчук С.О. Дослідження енергоефективності для мікросотових базових станцій 272

Бондаренко Е.И., Кравчук С.А. Исследование процедуры передачи обслуживания в беспроводных сетях с учетом требований к мобильности и нагрузке 275

Малецький Д.В., Кравчук С.О. Транспортні безпроводові мережі для систем мобільного зв'язку 5-го покоління..... 278

Рак Р.І., Кравчук С.О. Исследование процесса передачи обслуживания в микросотовых сетях стандарта LTE с использованием интерференционной координации 281

Казачінер К.А., Кравчук С.О. Підтримка мобільності в гетерогенних мережах широкосмугового доступу 284

Семендяк Є.С., Кравчук С.О. Передача обслуговування в WIMAX/LTE на базі IMS-архітектури 287

Кравчук С.О., Міночкін. Д.А., Рибак О.О. Можливості застосування «ХМАРНИХ» технологій в телекомунікаційних системах 290

Кибенко А.В., Міночкін Д.А. Використання сервісу DBAAS платформи OPENSTACK для створення баз даних для операторів мобільного зв'язку 293

Заєць І.О. Міночкін Д. А. Вертикальна передача обслуговування в безпроводових мережах 296

Ляшенко О. В., Кравчук С. О. Кооперативне рознесення сигналів в системі радіозв'язку 299

Кравчук С.О. Схема управління доступом до радіоканалу для MESH-мережі на основі аероплатформи 302

Кравчук С.О. Портативна тропосферна радіорелейна станція зв'язку. 305

Кайденко М.М., Кайденко В.М., Кравчук С.О., Роскошний Д.В. Модемний пристрій для тропосферної радіорелейної станції 308

Діденко І.В., Кравчук С.О. Канальна оцінка та адаптивна модуляція в системах когнітивного радіо 312

Секція 5. Інформаційні технології в телекомунікаціях

Співголови: д.т.н., проф. Глоба Л.С., к.т.н. Стрижак О.Є.,
к.т.н., доц. Скулиш М.А.

Доповідачі:

Рабченюк С.І., Прус Р.Б. Аналіз процесу впровадження хмарних технологій у світі 315

Алєксєєва К.І., Толюпа С.В. Використання інтелектуальних технологій у процесі управління інцидентами інформаційної безпеки 318

Дмитрук В.Р., Толюпа С.В. Захист інформаційних ресурсів від внутрішніх загроз 321

Федюнін С.А. Аналіз потоків відмов багатовимірних мереж. 324

Міхєєв Ю. І., Чернявський Г. П., Пінчук О. І., Шапар М. В. Вимоги до системи протидії негативному інформаційно-психологічному впливу . 327

Вдовенко Е.А., Воропаева А.А., Игнатьева В.Ю. Использование облачных технологий в контексте новых услуг в 3G сетях операторов мобильной связи 330

Шевченко О.В. Дослідження моделі поточного стану компонентів комп'ютерної мережі 333

Сиренко А.И. Использование виртуализации в задачах определения параметров производительности компьютерных систем 336

Зіменко Л.М. Забезпечення структурної живучості системи надання інтелектуальних послуг 339

Демидов І.В., Шпур О.М. Впровадження хмарних сервісних систем в національному мережному сегменті України 342

Климаш М.М., Селюченко М.О., Панченко О.М. Система моніторингу пакетної затримки в програмно-конфігурованих телекомунікаційних мережах 345

Лаврів О.А., Колодій Р.С., Хархаліс З.М., Мосоров В.Я. Моделювання DDoS-атаки на ВЕБ сервер 348

Слепец Ю.Ю., Гаттуров В.К. Применение концепции облачных вычислений к построению мобильных сетей на основе IP MULTIMEDIA SUBSYSTEM 351

Слепец Ю. Ю., Гаттуров В. К. Программная реализация надстройки IP MULTIMEDIA SUBSYTEM AS A SERVICE с помощью STAGED-EVENT DRIVEN ARCHITECTURE 354

Кривенко А. С., Штогріна О. С., Терновой М. Ю. Метод розподілення ієрархічного метаграфа на рівні 357

Репік С. І., Штогріна О. С. Методи розпізнавання тексту 360

Шемшур Я. С., Штогріна О. С. Розпізнавання елементів обличчя людини на зображенні 363

Косовненко Р. А., Штогрина О. С. Интеллектуальная технология оценки психофизического состояния человека 366

Воронюк М.М., Курдеча В.В., Плётка Б.С. Использование RASPBERRY PI для внедрения дополнительного функционала в сенсорной сети 369

Суліма С. В., Скулиш М.А. Алгоритм відображення та планування віртуалізованих функцій в мережі мобільного зв'язку 372

Федяй Я.І., Новогрудська Р.Л. Інформаційно - комунікаційне середовище співробітників антарктичного центру 375

Новогрудская Р.Л., Заика А.В. Системы BIG DATA, основные понятия 378

Бугаєнко Ю.М. Спосіб обробки інформації в вузлах IoT для зменшення навантаження на сервер обробки інформації 381

Кирюшкин Р.А., Курдеча В.В. Мультикритериальный метод вертикального хендовера 384

Лящук А. А., Міночкін Д. А. Використання технології MAAS для побудови «ХМАРНОГО» ДАТА-центру 387

Кривошеїна А.В., Міночкін Д А. Підвищення ефективності використання радіоінтерфейсу на базі MSC AXE-810 387

Алєксєєв М. О., Безлюднов Д. Є. Визначення аномальних станів у роботі пристроїв інтернету речей 390

Алексеев Н.А., Мазанка Р.М. Аутентификация в распределенных гетерогенных системах с динамической архитектурой 396

Глоба Л.С., Омельченко А.І. Організація взаємодії порталів НАНЦ та NASA на базі REST-сервісу 399

Алєксєєв М.О., Гусак О.В. Класифікація алгоритмів балансування навантаження для використання в розподілених гетерогенних мережах ... 402

Гончарова С. В., Могилевич Д. І. Алгоритм додаткового криптографічного захисту голосових даних 405

Ткачук А. О., Могилевич Д. І. Захист голосових даних в програмно-апаратному комплексі ASTERISK 408

Виговський М.С., Романов О.І. Сервіс IFTTT обчислень для розумного будинку 411

Омельченко Р.Ю., Романов О.І. Система розподілених GRID 414

Секція 6. Сенсорні мережі та прикладні аспекти застосування телекомунікаційних технологій

Співголови: д.т.н., проф. Лисенко О.І., д.т.н., проф. Романюк В.А

Доповідачі:

Давидюк В.О., Дакаєв О.В., Димид М.Д. Захищені безпроводові мобільні сенсорні мережі для моніторингу параметрів навколишнього середовища 417

Давидюк В.О., Петрова В.М. Забезпечення стійкості пропускної здатності безпроводової сенсорної мережі 420

Бендасюк Н., Прищепа Т.О. VHF і UHF антена для наносупутника 423

Бондарук О.А., Петрова В.М. Аналіз енергоспоживання вузла безпроводової сенсорної мережі 426

Живков А.П., Студенюк Р. Ю. Метаматериалы и связанные с ними процессы 429

Товкач И.О., Жук С.Я. Рекуррентный алгоритм пассивной локации в сенсорной сети по разностно-дальномерному методу при некоррелированных ошибках измерений. 432

Зайцев О.В. Модель розподілу ресурсів сенсорної мережі на основі модифікованого генетичного алгоритму 435

Зубик С. О. Способи захисту інформації в мобільних мережах 438

Кашуба С.В., Лисенко О.І. Гібридний метод визначення координат вузлів безпроводової сенсорної мережі 441

Кутельова О.С., Великий О.О. Метод адаптації безпроводових сенсорних мереж побудованих на радіогідроакустичних буях до умов функціонування 444

Новиков В.И., Лысенко А.И. Метод адаптивного управления маршрутизацией в условиях нестабильности связей между узлами беспроводной сенсорной сети 447

Остапенко О.О., Романюк В.А, Жук А.В. Аналіз методів та протоколів управління в беспроводних сенсорних мережах 450

Остапенко С.О., Прищепа Т.О. Використання платформи NODE.JS для розробки сучасних ВЕБ-сервісів 453

Piestova I.A., Andreiev A.A. Deep learning methodology adaptation for hyperspectral imagery classification 456

Поліник С.А. Моделювання бездротових сенсорних мереж 459

Прищепа Т.О., Лисенко О.І. Метод підвищення пропускної здатності мобільних сенсорних мереж з телекомунікаційними аероплатформами.... 462

Романюк А.В., Лисенко О.І. Використання інтелектуальних систем управління в сенсорних мережах із мобільними сенсорами 465

Семініченко В. В., Алєксєєва І.В. Покриття в безпроводових сенсорних мережах 468

Стрихалюк Б.М., Климаш Ю.В. Маршрутизація з гарантованою доставкою в 3D безпровідних сенсорних мережах 471

Тарасюк В.О. Надійний протокол маршрутизації для сенсорної мережі.. 474

Tachinina O., Chekanova I., Lysenko O., Alekseeva I., Chumachenko S. The system of injection of subminiature satellites (NANOSATELLITES) to NEAR-EARTH orbit on the basis of AH-124-100 airplane 477

Томашевська Т.В., Гордійко Н.О., Прищепа Т.О., Лисенко О.І. Метод використання геометричних фракталів для розв'язання задачі оптимального розміщення сенсорів при екологічному моніторингу 480

Трач Б.В., Лисенко О.І. Швидка оптимізація Ліпшица у безпроводових сенсорних мережах 483

Туранська О.С. Прищепа Т.О. Способи підвищення надійності безпровідних сенсорних мереж..... 486

Хоменко Є.О., Валуйський С.В. Підходи реагування на надзвичайні ситуації із застосуванням безпроводових сенсорних мереж 489

Шоферівський А. С., Курдеча В. В. Трирівнева архітектура взаємодії IoT пристроїв..... 492

Шпанчук О.О. Побудова найкоротшого розкладу збору даних у безпроводовій сенсорній мережі з обмеженим критичним енергоспоживанням..... 495

Явіся В.С. Методи забезпечення стійкої роботи сенсорних мереж на базі безпілотних літальних апаратів..... 498

Явіся В.С. Методика вибору мовних кодеків..... 501

Явіся В.С. Метод підвищення абонентської ємності систем мобільного зв'язку..... 504

Явися В.С. Способы управления пространственным положением наноспутника 507

Секція 7. Засоби та пристрої телекомунікацій

Співголови: д.т.н., проф. Трубін О.О., к.т.н., доц. Шелковніков Б.М.

Доповідачі:

Чумак Г.Л. Частотно-загороджувальний фільтр 3-см діапазону на основі магнітодіелектричного резонатора з природного магнетика..... 511

Шарко В. П. Предельное разрешение пространственных сигналов навигационных спутников алгоритма Кейпона 514

Печора М. О., Курінний О.К., Шелковніков Б.М. Розробка компланарного підсилювача потужності міліметрового діапазону..... 517

Шевченко А.Л., Радченко А.А., Шелковников Б.Н. Шевченко А.Л., Радченко А.А., Шелковников Б.Н. Разработка усилителя мощности миллиметрового диапазона на основе КМОП технологии..... 520

Курінний О.К., Печора М.О., Шелковніков Б.М. Розробка змішувача міліметрового діапазону 523

Радченко А.А, Шевченко О.Л., Шелковніков Б.М. Разработка малошумящего усилителя миллиметрового диапазона 526

Авдєєнко Г.Л., Корсак В.В., Якорнов Є.А. Модифікація алгоритму Кейпона для визначення пеленгу на джерела радіовипромінювання при сферичних фронтах їх електромагнітних хвиль у місці прийому..... 529

Авдєєнко Г.Л., Корсак В.В., Якорнов Є.А. Моніторинг радіовипромінювання в ближній і проміжній зонах на основі алгоритму Кейпона 532

Бунін С.Г., Авдєєнко Г.Л., Михайлов С.О. Побудова системи надширокосмугового зв'язку у діапазоні 200-400 МГц 535

Половий О.М, Приступчук Ю.А., Шелковніков Б.М. Разработка удвоителя миллиметрового диапазона..... 538

Воловик А.О., Бунін С.Г. Апроксимація характеристик радіолінії доступу в сантиметровому і дециметровому діапазонах..... 541

Секція 8. Підготовка кадрів телекомунікаційного профілю, історія розвитку телекомунікацій.

Секцію 8 об'єднано з Секцією 2.

Секція 9. Modern information and telecommunication trends

Співголови:
д.т.н., проф. Бунін С.Г., Назаренко О.І., д.т.н., проф. Уривський Л.О.

Доповідачі:

Hakhova H. Latvian experience: The comparative review of study abroad via the ERASMUS+ programme 544

Kurdecha V. V., Ishchenko I. I., Zakharchuk A. G. Data processing and storage in the Internet of things systems..... 546

Kurdecha V.V., Gvozdetska N.A., Zvonarov O.V. The internet of things (IoT) systems containing nomadic units architecture modification and the most rational technologies selection 549

Svetsinskaya E.S., Sunduchkov K.S. Borders calculation of optimization parameters changes at synthesis of a satellite distribution network 552

Drobina O.S., Avdeyenko G.L., Naritnik T.M., Naboka B.Y. Digital radio signals transmission of DVB-T and DVB-T2 standards by using terahertz frequency - band radio channel..... 555

Chernyavsky A. A., Pilipenko A. A. SaaS virtualization method and ITS application 558

Восьма Міжнародна науково-технічна конференція студентів та аспірантів «ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА СИСТЕМ»

Співголови:

ЯКОРНОВ Є.А. – заступник директора інституту телекомунікаційних систем НТУУ «КПІ», к.т.н., професор;

ЛАЗАРЕНКО О.П. – голова студентської ради інституту телекомунікаційних систем НТУУ «КПІ».

Засідання 1.
Доповідачі:

Ахтирцева В.С. Методи генерування, поширення інформаційно-психологічних впливів у телекомунікаційних системах 563

Мажаренко Е.В. Реалізація серверу аудіо конференції на базі IP PBX FREESWITCH 564

Саенко Б. В. Защита информации в VIRTUAL PRIVATE NETWORK 564

Шевченко М.В. Возможные методы поддержания достоверности связи в протоколе 802.11N 565

Тимченко И.О. Доставка сигналов услуг по спутниковому радиоканалу в гетерогенной распределительной сети 566

Кузянин А.С. АРХИТЕКТУРА БЕЗОПАСНОСТИ ТЕХНОЛОГИИ INTERNET OF THINGS, IoT 566

Баженов П. О. Взаимосвязь ресурсов мультисервисной сети связи и ее информационных возможностей 567

Куклина А. С. Использование механизма EXPLICIT CONGESTION NOTIFICATION (ECN) для защиты сетей от перегрузки 568

Мєлєхова М.О., Білан А.М. Інтернет речей в сучасних телекомунікаційних мережах 568

Остапенко С.О. NODE.JS для розробки сучасних сервісів які працюють в режимі реального часу 569

Побута О.В. Реалізація функції відео конференції на базі IP PBX ASTERISK 570

Парадовский А.А. Система видеотелеметрии для геостационарного телекоммуникационного спутника 571

Найдич В.Р. Технологія реалізації стратегій передачі інформації в LAN 572

Омельченко Р.Ю. Застосування ГРІД - систем для вирішення складних обчислювальних задач 573

Лящук А.А. Переваги використання платформи OPENSTACK Для побудови інфраструктури як сервісу (IAAS) 574

Кибенко А.В. Процес аутентифікації і авторизації для послуг OPENSTACK 574

Бабич М.В. Алгоритм взаємодії протоколів SIP і ОКС№7 в телекомунікаційних мережах на базі SOFTSWITCH 575

Сапа Т.И. Проверка чистоты торцов волокна и их очистка 576

Дмитриєв В.В. Аналіз параметрів VOIP мережі, які впливають на якість передачі голосу 576

Буглак Д. А. Налаштування VOIP мережі на базі ASTERISK 577

Осипчук И. С. Исследование мультисервисной сети связи на основе стандарта 802.11N 578

Бугаєнко Ю.М. Вирішення проблеми злиття даних в IoT за допомогою архітектури JOINT DIRECTOR OF LABS 579

Похилинский С.А. Модифицированная архитектура сети INTERNET OF THINGS за счет использования репрограммируемого микроконтроллера 580

Бовтрук А. Ю. Порівняльний аналіз технологій надання широкосмугових послуг на базі технології MPLS 581

Пленарні доповіді

УДК 621.372

ИНВЕРСИЯ МОД КОЛЕБАНИЙ В ЯЧЕЙКАХ МЕТАМАТЕРИАЛОВ

Ильченко М.Е., Живков А.П.
Институт телекоммуникационных систем НТУУ «КПИ», Украина
E-mail: zhivkovalex@gmail.com

Inversion oscillation modes in metamaterials cells

Metamaterials are considered separate cell. Their representation in the form of various types of microwave resonators allowed the authors to obtain results that allow to explore and simulate such a cell on the basis of oscillatory systems - oscillators and rotators.

С момента появления в 1999 году статьи [1], которую принято считать основополагающей в части практической реализации метаматериалов, число публикаций на эту тему стремительно возрастает. Появились и работы, обобщающие проведенные исследования, такие, например, как [2]. Однако по-прежнему актуальной остается проблема выработки боле-менее общей терминологии для описания и изучения подобного рода структур, особенно в связи с тем, что метаматериалы активно завоевывают свои позиции и в акустике, и в процессах (возможно целесообразно использовать здесь термин - метапроцессы). Это и эффекты Вавилова-Черенкова и Доплера, и такое широко известное явление, как мираж. Едва ли можно при изучении акустических свойств метаматериалов пользоваться понятиями магнитного и электрического диполей, хотя зачастую процессы, происходящие в электродинамических и акустических метаматериалах, описываются одинаковыми или похожими математическими уравнениями и моделями. В начале своего монументального труда «Лекции по теории колебаний» [3] академик Л.И Мандельштам, который по праву считается одним из «родоначальников» изучения сред с отрицательным коэффициентом преломления, отметил, цитируя Планка: «правильная классификация – это уже высокий вид познания».

С проблемой правильной классификации и общей терминологии пришлось столкнуться и авторам [4], которые в конце 80-х – начале 90-х годов прошлого века активно исследовали (и публиковали результаты исследований) структуры, подобные ячейкам метаматериалов, такие как как режекторные и полосовые фильтры с двумя или несколькими резонаторами, не связанными между собой и расстроенными в общем случае по частоте.

Не претендуя на всеобщность и единственность подхода, мы бы хотели обратить внимание на те элементарные структуры (ячейки) метаматериалов, в которых в явном виде реализованы или «угадываются» резонаторы или колебательные системы, то есть по возможности перейти к использованию понятий «синфазных» и «противофазных» колебаний [5], «осцилляторов» и «ротаторов» [6]. Это, как нам кажется, позволит выявить некоторые

принципиально важные свойства метаматериалов и метапроцессов.

Понятие синфазных и противофазных колебаний возникло при изучении связанных колебаний. Система связанных резонаторов характеризуется парциальными и нормальными частотами [5]. Парциальные частоты – это резонансные частоты независимых колебательных систем (отдельных резонаторов, вырожденных колебаний резонаторов сложной формы…), которые не связаны между собой. Нормальные частоты (моды) - характерны для системы связанных резонаторов, они составляют колебательный спектр системы. Колебание физической системы является суперпозицией нормальных колебаний.

Нормальные колебания могут быть рассмотрены как синфазные и противофазные колебания, модель которых в виде связанных маятников представлена на рис. 1:

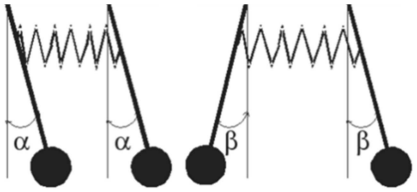


Рис. 1 Модель синфазных а) и противофазных б) колебаний.

Из [7] следует, что частота синфазных колебаний $f_{\text{сф}}$ всегда ниже частоты противофазных колебаний $f_{\text{пф}}$. Это является принципиально важным для всякого рода «натуральных материалов», «строящихся» на базе связанных колебаний.

Вернемся к «электрическим» и «магнитным» типам колебаний, при рассмотрении метаматериалов такой подход использован, например, в [8]. Рассмотрим элементарную ячейку метаматериала, как это сделано в [4]. На рис. 2 представлены два варианта ячеек метаматериалов - традиционная в виде двух разомкнутых колец резонаторов и ее аналог в виде полосковых резонаторов с длинами, близкими к λ/2 и λ соответственно (здесь λ –длина волны, соответствующая резонансной частоте ячейки метаматериала, которая лежит между парциальными частотами резонаторов (колебаний), образующих ячейку и примерно равна (fэ + fм)/2 (здесь fэ и fм - резонансные частоты электрического и магнитного типов колебаний соответственно).

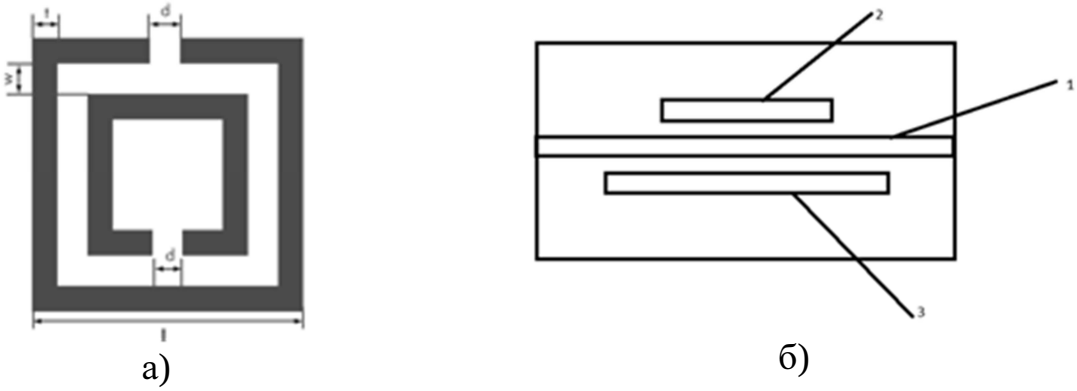


Рис. 2 Ячейки метаматериалов в виде а) двух разомкнутых колец, лежащих в одной плоскости и б) «полуволнового» (2) и «волнового» (3) резонаторов.

«Внутренний» резонатор на рис. 2 а) и «полуволновый» резонатор на рис. 2 б) соответствуют «магнитному» (магнитный диполь) типу колебаний, а «внешний» резонатор на рис. 2 а) и «волновой» резонатор на рис. 2 б) соответствуют «электрическому» типу колебаний (электрический диполь). Структуры, подобные приведенным на рис 2 б, обладают свойствами метаматериала («неминимальнофазовость», которую можно трактовать как направленность фазовой и групповой скоростей навстречу друг другу…) в том случае, если fэ > fм. В терминологии синфазных и противофазных колебаний [4] это означает, что $f_c > f_{\text{пф}}$, что *принципиально* невозможно для структур, построенных на связанных колебаниях, но вполне реализуемо в искусственно создаваемых ячейках метаматериалов. Это их фундаментальное свойство и фундаментальное отличие от «натуральных» материалов.

В таблице 1 сделана попытка классификации типов колебаний по их фазовым портретам [6]. Разумеется, она довольно условна, но в дальнейшем позволит проводить некоторые аналогии между метаматериалами в эдектродинамике, акустике, и «метапроцессами».

Таблица 1.

Колебательная система	**Тип**	**Синфаз-ность**	**Аналог диполя**
1. Электрон	Ротатор	+	Электрический
2. Колесо (строб-эффект)	Ротатор	+	Электрический
3. «Полуволновой резонатор»	Ротатор	+	Электрический
4. Колебания ДР $E01^{\delta}$ типа	Ротатор	+	Электрический
5. Моргающий фонарь (для демонстрации строб-эффекта)	Осциллятор	-	Магнитный
6. Маятник, качели	Осциллятор	-	Магнитный
7. «Волновой» резонатор	Осциллятор	-	Магнитный
8. Колебания ДР $H01^{\delta}$ типа	Осциллятор	-	Магнитный

Поскольку, ка отмечалось, в ячейках метаматериалов отсутствуют связанные между собой колебания, естественно полагать, электромагнитной волны в них также определяется не связанными между собой колебаниями, как, например, в нормальных диэлектрических средах, а происходит подобно распространению волны в волноведущих структурах (волновод, оптоволокно…). Об этом свидетельствует и модель магнитоиндукционных волн (МИ-волны), детально описанная в [2], и волны в так называемых омега-структурах [9].

Подводя итоги доклада, можем сделать следующие выводы относительно специфических свойств метаматериалов:

1. Присущие базовым ячейкам метаматериалов колебания не связаны между собой и принципиально относятся к разным типам (синфазные и противофазные, электрические и магнитные, ротатор и осциллятор).
2. Для достижения «неминимальнофазовости», обеспечивающей встречное направление групповой и фазовой скоростей, необходимо выполнение соотношения между частотами колебаний fэ > fм ($f_c > f_{\text{пф}}$), что принципиально недостижимо в материалах, в которых волна распространяется благодаря связанным колебаниям одинаковых структур.
3. Электромагнитная волна в магнитоматериальной среде распространяется как в среде волноведущей, без «помощи» связанных колебаний.
4. В хорошо известном строб-эффекте (кажущееся вращение колеса в обратную сторону в фильмах или при подсветке его мигающим источником света) частота ротатора (вращения колеса) больше частоты осциллятора (источника света). Этому вопросу, как и акустическим метаматериалам (в терминах колебательных систем) посвящен отдельный доклад.

В качестве гипотезы следует отметить, что при существовании неких материалов, в которых могут существовать близко (в сравнении с длиной электромагнитной волны в структуре) расположенные «источники» колебаний, аналогичные по своим свойствам электрическому и магнитному диполям, такие среды могут проявлять свойства метаматериалов. Наиболее вероятная «среда» их обитания – кристаллы в пока еще мало освоенном террагерцевом диапазоне.

Литература

1. J. B. Pendry, A. J. Holden, D. J. Robbins, and W. J. Stewart. “Magnetism from Conductors and Enhanced Nonlinear Phenomena», IEEE Transactions on Microwave Theory and Techniques, vol. 47, No. 11, November 1999
2. Metamaterials Handbook: Vol. I. Phenomena and Theory of Metamaterials. 926 p. Vol. II. Applications of Metamaterials. 724 p. / Ed. by F. Capolino CRC Press, Taylor & Francis Group, 2009.
3. Мандельштам Л.И. Лекции по теории колебаний. М. - Наука. - 1972 г.
4. Ильченко М.Е., Живков А.П., Орлов А.Т. Фильтры на базе резонаторов с близкими по частоте модами как ячейки метаматериалов.// Наукові вісті НТУУ «КПІ». – 2016. – № 1 (104). – С. 7–14.
5. М. И. Рабинович, Д. И. Трубецков. Введение в теорию колебаний и волн. – М.- "Наука," Глав. ред. физико-математической лит-ры, 1984. - 431 стр.
6. А. Зоммерфельд. Строение атома и спектры. Том. 1. Государственное издательство технической литературы. - М.- 1956 г.
7. Пиппард А. Физика колебаний.- М.- Высшая школа,-1985.-456 с.
8. I.B. Vendik, O.G. Vendik and M.A. Odit: Physics of the Solid State Vol. 51 (2009), p. 1590.
9. «Bianisotropic route to the realization and matching of backward-wave metamaterial slabs» S. A. Tretyakov, C. R. Simovski, and M. Hudlička Phys. Rev. B 75, 153104 – Published 24 April 2007.

UDC 621.396.946

SCATTERING OF ELECTROMAGNETIC WAVES ON DIFFERENT DIELECTRIC RESONATOR STRUCTURES

Trubin A. A.
National Technical University of Ukraine "Kyiv Polytechnic Institute"
E-mail: atrubin@ukrpost.net

РОЗСІЮВАННЯ ЕЛЕКТРОМАГНІТНИХ ХВИЛЬ НА СТРУКТУРАХ РІЗНИХ ДІЕЛЕКТРИЧНИХ РЕЗОНАТОРІВ

Проведено узагальнення електродинамічної теорії розсіювання електромагнітних хвиль лінії передачі на системах відмінних по формі та діелектричної проникності діелектричних резонаторів. Досліджені частотні залежності матриці розсіювання смугових та режекторних фільтрів, побудованих на різних формах ДР.

In constructing the theory supposed that all resonators have the same form and consists from the same dielectric. To improve the parameters in some cases there is need to build filters on different form DRs made from variant dielectrics. However, in this case it becomes much more complicated theory, describing scattering processes on such structures. We find the system of equations, describing different DR structures. Found total solution. In the special case of identical resonators obtained solution becomes known [1].

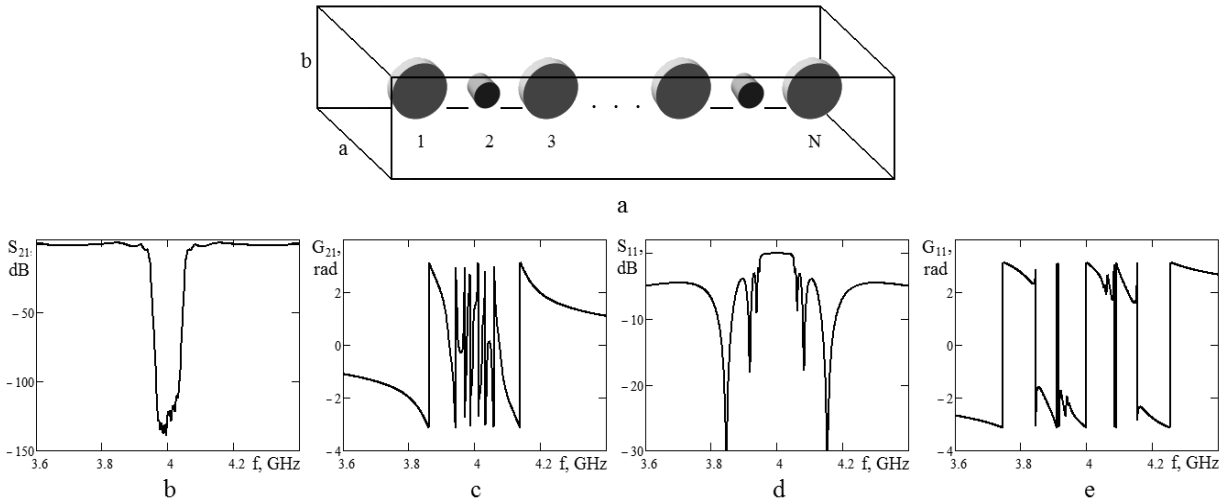


Fig. 1. Different Cylindrical DR structure on the symmetry axis of propagating Rectangular metal waveguide (a). S-parameters (b - e) of the bandstop filter on 9 Cylindrical DRs with $\varepsilon_{1r} = 36;\ \varepsilon_{2r} = 82.$

Using obtained equations we present here the results of the study process of the scattering of electromagnetic waves on the different DR structures in the

propagating waveguide as well as evanescent waveguide segment. It is assumed that all the resonators are excited by the main type of natural oscillations of the magnetic type.

Fig. 1 shows scattering parameters of the bandstop filter, consisting of 5 Cylindrical DRs characterized by the dielectric permittivity $\varepsilon_{1r} = 36$ and by the relative size $\Delta_1 = L_1 / 2r_1 = 0{,}4$ as well as 4 DRs with $\varepsilon_{2r} = 82$; $\Delta_2 = L_2 / 2r_2 = 0{,}8$. Here $2r_s$ - is the diameter; L_s - is the height of the s-th DR ($s = 1, 2$). The distance between the centers of adjacent DRs was equal to $\lambda_w / 4$, where λ_w - is the waveguide number.

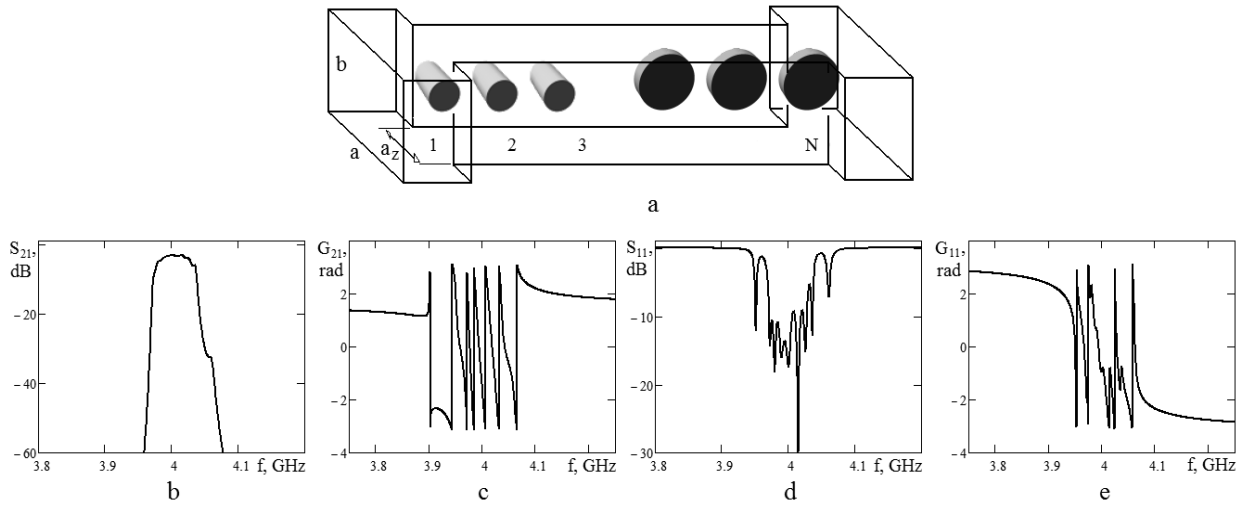


Fig. 2. Cylindrical DR on the symmetry axis of evanescent Rectangular metal waveguide segment (a). S-parameters of the bandpass filter on 11 Cylindrical DRs with $\varepsilon_{1r} = 36$; $\varepsilon_{2r} = 82$.

The best results were obtained for the DR structures located in the evanescent waveguide segment and forming bandpass filter. It's desirable the filters containing the DR should have a clean bands free of spurious oscillations. The solution of this

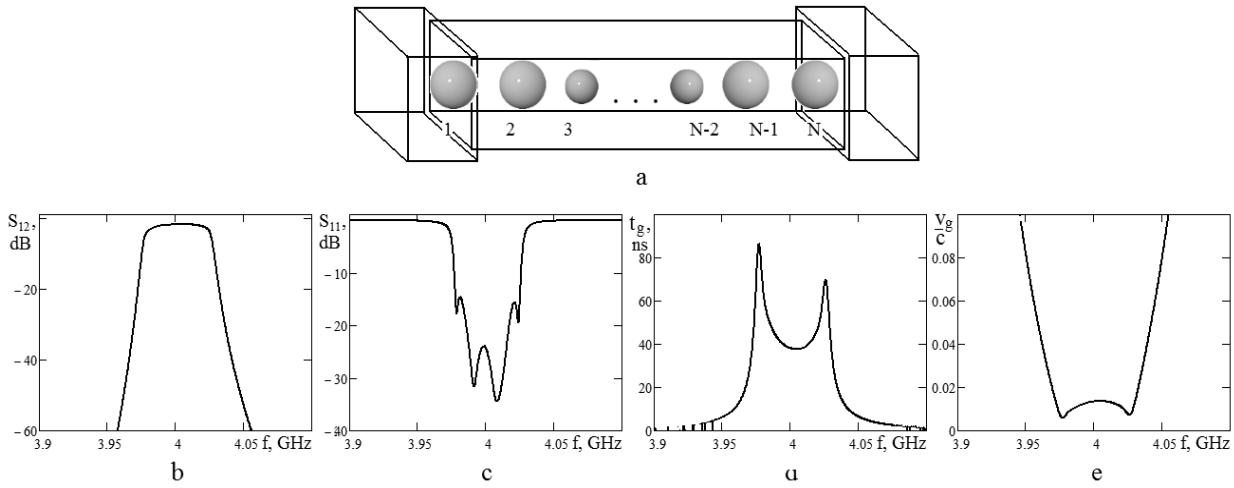


Fig. 3. Different Spherical DRs in the evanescent Rectangular metal waveguide segment (a). Scattering parameters of the bandpass filter on 11 Spherical DRs with $\varepsilon_{1r} = 36$; $\varepsilon_{2r} = 82$.

problem is known possible using different DRs.

Fig. 2 shows scattering parameters of the filter, consisting of two lattices different Cylindrical DRs. First lattice containing 4 DR with $\varepsilon_{1r} = 36,\ \Delta_1 = 0{,}8$, the second lattice consists from 7 DR with $\varepsilon_{2r} = 81,\ \Delta_2 = 0{,}4$. The distance between the centers of adjacent first type DRs was equal to 17 mm; for the second type DRs 21 mm.

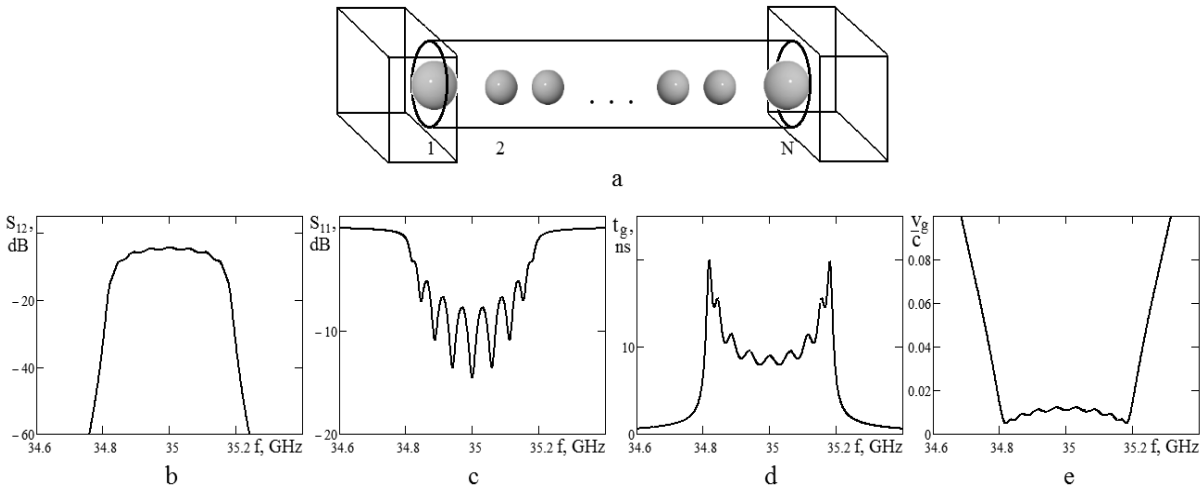


Fig. 4. Different Spherical DRs in the evanescent Cylindrical metal waveguide segment (a). Scattering parameters of the bandpass filter on 11 Spherical DRs with $\varepsilon_{1r} = 36;\ \varepsilon_{2r} = 82$.

The use of different Spherical DRs also could improves the filter parameters. Fig. 3 shows 8 DR bandpass filter scattering matrix. Recent resonators filter made of dielectric with $\varepsilon_{1r} = 36,\ Q_1^D = 3000$, the rest are made of dielectric $\varepsilon_{2r} = 81$, $Q_2^D = 2000$. All resonators form symmetrical structure. The distance between the centers of first and second DR is 23,5 mm, among other DRs is 20 mm. The cross section of the input and output waveguides $a \times b = 58 \times 25 mm^2$, the cross section of the evanescent waveguide $az \times bz = 20 \times 25 mm^2$.

Fig. 4 shows 11 Spherical DR arrangement in Circular Cylindrical metal waveguide. The cross section of the input and output waveguides $a \times b = 7 \times 3 mm^2$; the radius of the evanescent waveguide $Rz = 1{,}5 mm$.

Thus, the use of different DRs can greatly enhances design filters. As shown by preliminary calculations, the developed model correctly describes the scattering processes in the system of different DRs in a variety of transmission lines.

References

1. A.A. Trubin, Scattering of electromagnetic waves on the Systems of Coupling Dielectric Resonators, Radio electronics, №2, 1997, pp. 35-42.

INTERNET OF THINGS. ЧТО ЭТО ТАКОЕ, ПЕРСПЕКТИВЫ И РЕАЛИЗАЦИЯ

Андрей Дудченко
Компания Nokia, Украина
E-mail: olena.lobunets@nokia.com

Интернет вещей (англ. Internet of Things, IoT) — концепция вычислительной сети физических объектов («вещей»), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой, рассматривающая организацию таких сетей как явление, способное перестроить экономические и общественные процессы, исключающее из части действий и операций необходимость участия человека.

Концепция сформулирована в 1999 году как осмысление перспектив широкого применения средств радиочастотной идентификации для взаимодействия физических объектов между собой и с внешним окружением. Наполнение концепции «интернета вещей» многообразным технологическим содержанием и внедрение практических решений для её реализации начиная с 2010-х годов считается восходящим трендом в информационных технологиях, прежде всего, благодаря повсеместному распространению беспроводных сетей, появлению облачных вычислений, развитию технологий межмашинного взаимодействия, началу активного перехода на IPv6 и освоению программно-конфигурируемых сетей.

В докладе рассматривается концепция Интернета вещей, ее ключевые составляющие и потенциальные способы реализации.

УДК 621.396.4

ОСОБЛИВОСТІ СПОСОБІВ ОЦІНКИ ПРОДУКТИВНОСТІ МЕРЕЖІ НА ОСНОВІ 802.11ac

Уривський Л.О., Осипчук С.О., Шмігель Б.О.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: bshmigel@gmail.com

802.11ac network performance assessment peculiarities

The paper reviews wireless standard IEEE 802.11ac and equipment for wireless network based on this standard. We tested the network productivity in lab, specifically TCP data rate in point-to-point (PTP) wireless network based on SDR IEEE 802.11ac transceivers. We described the scenarios for wireless networks performance assessment and how they impact network performance: approaches for traffic load generation and respective consuming of SDR hardware computational resources.

Одним із найсучасніших стандартів безпроводового зв'язку IEEE 802.11 [1] є стандарт IEEE 802.11ac [2]. Актуальною задачею є оцінка енергетичних характеристик каналу та продуктивності, а саме – швидкості передачі даних в безпроводовій мережі передачі на основі прийомопередавачів 802.11ac. В роботі оцінка продуктивності мережі виду точка-точка проведена на основі використання обладнання Mikrotik RB/921UAGS-5SHPacT-N для радіорелейного зв'язку (РРЛ), що відповідає стандарту 802.11ac, в режимі передачі TCP трафіку (рис. 1).

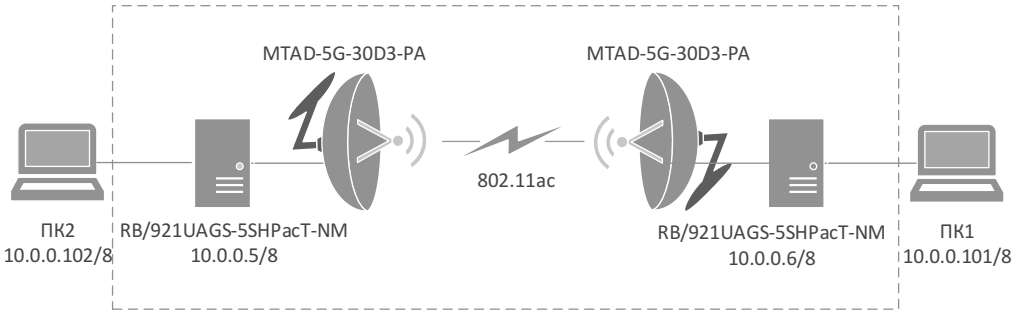


Рис. 1 Структурна схема організації мережі для оцінки продуктивності з використанням РРЛ обладнання Mikrotik RB/921UAGS-5SHPacT-N та антен MTAD-5G-30D3-PA.

Особливістю сучасних високошвидкісних безпроводових систем передачі є побудова прийопопередавачів на основі концепції SDR (software defined radio, – програмно-визначених радіосистем) [3]. При цьому дуже важливим фактором, що критично впливає на продуктивність мережі у разі високих швидкостей передачі, є швидкодія апаратної частини SDR системи.

Для забезпечення надійного каналу передачі даних використовується протокол TCP. Для отримання максимальної пропускної здатності каналу, в TCP пакеті повинен бути встановлений максимальний розмір блоку (MTU, 1500 байт для Ethernet). Чим більше MTU, тим менше витрат на передачу службової інформації, а тому – вища продуктивність каналу. Важливим

параметром TCP є також розмір вікна, який визначає максимальну кількість байт переданих даних, яку відправник може надіслати без отримання підтвердження про доставку. Метод визначення оптимального розміру вікна для TCP виходить за рамки роботи. При проведенні тестувань вибраний розмір вікна 64 кБ, що дозволяє отримати максимальну швидкість передачі.

При першому способі оцінки продуктивності мережі, використаний вбудований програмний інструмент WinBox для генерації потоку даних по протоколу TCP між прийомопередавачами, що показав максимально досяжну швидкість передачі TCP трафіку 140 Мбіт/с при заявлених виробником 866 Мбіт/с. Однак виявилось, що у разі застосування такого інструменту для оцінки продуктивності, навантаження на процесор прийомопередавачів досягає 100%, що пов'язано з необхідністю генерування та обробки пакетів. В результаті, такий спосіб оцінки продуктивності мережі, з генеруванням трафіку утилітою WinBox, не дозволяє достовірно отримувати характеристики мережі у зв'язку з обмеженням продуктивності апаратної частини SDR системи прийомопередавачів.

Іншим способом оцінки продуктивності мережі є застосування програмного забезпечення iperf на абонентських терміналах, що генерують TCP трафік, або ж передача файлу значного об'єму. При такому способі задача генерування трафіку покладається на обчислювальні ресурси абонентських терміналів, а ресурси прийомопередавачів задіяні тільки для передачі та приймання трафіку, що знижує кількість обчислювальних операцій в приймально-передавальних засобах SDR. В результаті оцінки продуктивності каналу зв'язку вказаним способом за схемою рис. 1, швидкість передачі з використанням протоколу TCP в одну сторону досягла 360 Мбіт/с. Однак заявлена виробником швидкість 866,6 Мбіт/с для використаного обладнання все ще не досягнута (рис. 2).

Як показано на рис. 2, при проведенні дослідження, безпроводовий канал мав наступні енергетичні характеристики: рівень вхідного сигналу: -21…-23 дБм, відношення сигнал/шум 79 дБ. Відповідно, за вказаних умов SDR система за заданим алгоритмом і критеріями вибирає найкращу сигнально-кодову конструкцію згідно стандарту 802.11ac, за якої повинна бути досягнута швидкість передачі даних в безпроводовому каналі 866.6 Мбіт/с [2]. В свою чергу, у стандарті 802.11ac два просторових потоки на 80 МГц, короткий захисний інтервал 400 нс і максимальна модуляція QAM-256 із завадостійким кодуванням 5/6 на 234 піднесучих OFDM повинні забезпечувати 866.6 Мбіт/с, але на практиці таку швидкість передачі даних досягнути не вдається, і найкращим результатом є досягнення середньої швидкості 360 Мбіт/с з тимчасовим збільшенням швидкості у певні моменти часу до 390 Мбіт/с.

Можна виділити наступні фактори, що призводять до зниження швидкості передачі у порівнянні із заявленою виробником швидкістю:

1. Службова інформація та заголовки пакетів, що передається між обладнанням 802.11ac;
2. Завадостійке кодування для запобігання помилок при передачі даних;

3. Повторна передача даних по протоколу TCP внаслідок некоректно прийнятих даних після перевірки контрольної суми.

Детальний аналіз надлишковості протоколу TCP проведено в [4,5].

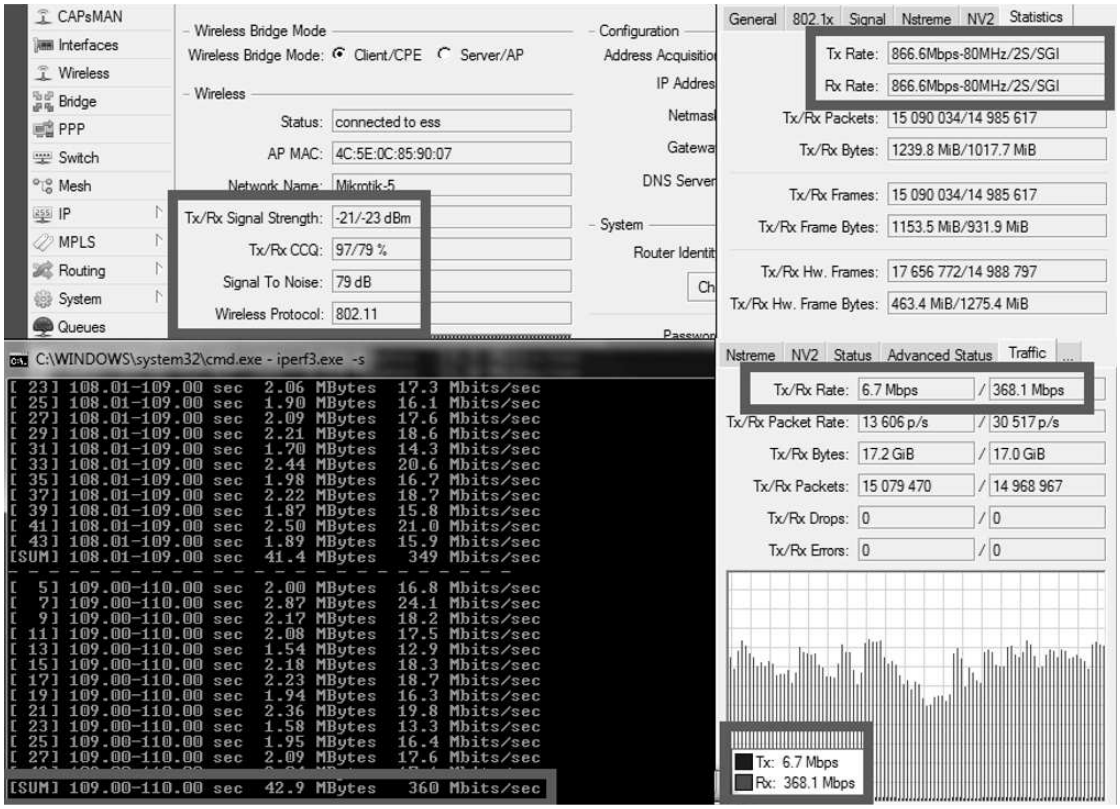


Рис. 2 Результати вимірювань швидкості передачі TCP трафіку в РРЛ з використанням утиліти iperf для генерування трафіку TCP.

Висновки. В роботі розглянуто способи оцінки продуктивності, а саме – швидкості передачі даних в безпроводовій мережі на основі обладнання 802.11ac при передаванні TCP трафіку. Відмічено особливості кожного способу оцінки продуктивності мережі. Експериментально досягнуто найкращу інформаційну швидкість для абонента 360 Мбіт/с при заявлених 866,6 Мбіт/с, що спричинено передаванням службової інформації та алгоритмами обробки даних при передачі.

Література

1. L. Usryvsky, S. Osypchuk, B. Shmigel. The 802.11 Protocols Usage for Wireless Systems Construction with Flexible Architecture. TCSET'2016, February 23–26, 2016, Lviv-Slavske, Ukraine. pp. 918-921.
2. Matthew S. Gast. 802.11ac: A Survival Guide. O'Reilly, 2013. – 152p.
3. Narytnik, L. Uryvsky, S. Osypchuk. Implementation of the Software Defined Radio Concept in Terahertz Range Based on Wi-Fi. – 2nd International Scientific-Practical Conference "Problems of Infocommunications. Science and Technology", IEEE PIC S&T 2015, 13 - 15 October, Kharkiv, Ukraine. – pp. 209-212.
4. G. Xylomenos, G. Polyzos, P.Mähönen, M. Saaranen. TCP Performance Issues over Wireless Links, 12 p.
5. О.М. Тарасюк, А.В. Горбенко, М.С. Газал. Анализ избыточности протоколв стека TCP/IP. Системи обробки інформації, 2009, випуск 1 (75), с.130-133.

УДК 621.396.1

СПЕЦІАЛЬНІСТЬ ТЕЛЕКОМУНІКАЦІЇ ТА РАДІОТЕХНІКА: НОВІ СПЕЦІАЛІЗАЦІЇ

Ільченко М.Ю., Кравчук С.О., Міночкін Д.А., Явіся В.С.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: sakravchuk@ukr.net

SPECIALTY TELECOMMUNICATIONS AND RADIO ENGINEERING: NEW SPECIALIZATIONS

New specializations specialty "telecommunications and radio engineering" based on years of experience training at the Department of Telecommunications NTUU "KPI" in the direction of "telecommunications" and achievements in scientific and technological research and development aimed at obtaining new knowledge, systems and technologies in the field of telecommunications.

Нові спеціалізації спеціальності «телекомунікації та радіотехніка» базуються на багаторічному досвіді підготовки спеціалістів на кафедрі телекомунікацій НТУУ «КПІ» з напряму «телекомунікації» і здобутках у проведенні науково-технічних досліджень та розробок, спрямованих на отримання нових знань, систем і технологій в сфері телекомунікацій [1]. Продукування нових наукових знань викладачами є постійним джерелом оновлення змісту освіти через формування нових навчальних спеціалізацій. А на цьому базисі – створення на інноваційних засадах нових технологій і техніки. Зазначені тенденції сприяють тому, що у формуванні змісту професійно-орієнтованих навчальних дисциплін усіх спеціалізацій використовуються оригінальні наукові результати науковців Інституту телекомунікаційних систем.

Спеціалізація «Мобільні телекомунікації». Головною тенденцією розвитку сучасних телекомунікацій є забезпечення якісних комунікацій обміну інформацією для будь-яких користувачів або інтелектуальних машинних об’єктів незалежно від місця їх розташування та швидкості руху. При цьому користувачі повинні мати повну незалежність і свободу переміщення, тобто – мобільність. Конвергенція технологій, систем та послуг дозволяє поширити підтримку мобільності на всю інфраструктуру телекомунікацій і таким чином вийти на новий сучасний рівень їх розвитку – мобільних телекомунікацій.

Спеціалізація «Мобільні телекомунікації» забезпечує фундаментальну, прикладну і практичну підготовку на трьох рівнях вищої освіти - бакалавр, магістр, доктор філософії у галузі знань «електроніки та телекомунікацій», спеціальності «Телекомунікації та радіотехніка», яка дозволяє опанувати основами цифрових комунікацій; програмної інженерії; побудови, телекомунікаційних систем і мереж з підтримкою мобільності.

Центральне місце в спеціалізації займає опанування методами підтримки мобільності в сучасних стільникових системах радіодоступу, в тому числі 5-го покоління, системах широкосмугового доступу, неоднорідних багаторівневих телекомунікаційних розподілених мережах на базі різних технологій та архітектур. Спеціалізація дає поглиблені знання щодо налагодження, функціонування і експлуатації телекомунікаційних систем та адміністрування ними. Надає можливість опанування сучасною доктриною розвитку телекомунікацій - розумних всепроникних мереж.

Рівень бакалавра забезпечений підготовкою наступними блоками дисциплін: Основи теорії цифрового зв'язку, Програмні інструменти телекомунікацій, Системи телекомунікацій та управління, Мобільні телекомунікації, Регулювання в телекомунікаціях. З досягненням даного рівня випускник матиме компетенцію зі створення систем та мереж телекомунікацій, їх використання та обслуговування.

Рівень магістр забезпечений підготовкою комплексним блоком дисциплін мобільних телекомунікацій, що дозволяє опанувати основи підтримки мобільності, системи широкосмугового доступу, теорію прийняття рішень та системний аналіз, проектування та моделювання телекомунікаційних систем, організацію наукових досліджень та управління проектами в телекомунікаціях, адміністрування телекомунікаційних серверів та мереж, захист інформаційних ресурсів. Крім цього надаються знання із принципів побудови мереж оператора мобільного зв'язку як складової частини розумних всепроникних мереж. З досягненням даного рівня випускник матиме компетенцію з розробки, побудови і управління гетерогенними телекомунікаційними мережами та методами підтримки в них мобільності.

Рівень доктор філософії у напрямку електроніки та телекомунікацій забезпечений підготовкою комплексним блоком дисциплін докторської програми мобільних телекомунікацій, що дозволяє опанувати організацію наукової діяльності за докторською програмою, математичне моделювання систем та процесів, сучасні тенденції розвитку мобільних телекомунікацій, мистецтво побудови високошвидкісних телекомунікацій, тенденції розвитку розумних всепроникних мереж, створення інноваційно-наукових стартапів в сфері мобільних телекомунікацій.

Спеціалізація «Апаратно-програмні засоби електронних комунікацій». Практично всі аспекти людської діяльності пов'язані з обміном інформацією, що не можливо без сучасних засобів електронних комунікацій, які складають основу новітніх телекомунікаційних систем. Зростання попиту на комунікаційні послуги, розвиток систем і технологій телекомунікацій вимагає постійного удосконалення відповідних засобів: від простих електронних пристроїв - до складних апаратно-програмних комплексів, що вирішують не тільки задачі безпосереднього прийому, передачі, обробки і відтворення інформації, а також збільшення гнучкості, продуктивності та надійності при створенні різноманітних програмованих структур комунікацій. Крім цього сучасний розвиток галузі телекомунікацій характеризується зростанням її конвергенції з комп'ютерними та

інформаційними технологіями і, як наслідок, все більшим наповненням телекомунікаційних систем програмними засобами. Дана тенденція та потреба в прискоренні процесів створення та реалізації таких засобів вказує на необхідність підготовки фахівців, що володітимуть не лише знаннями зі створення та експлуатації засобів електронних комунікацій, розповсюджених загальних засад програмування, а й знаннями з реалізації спеціалізованих програмних засобів обробки даних для телекомунікацій.

Спеціалізація «Апаратно-програмні засоби електронних комунікацій» забезпечує фундаментальну теоретичну, прикладну і практичну підготовку за загальною програмою галузі знань «Електроніка та телекомунікації», спеціальності «Телекомунікації та радіотехніка» на трьох рівнях вищої освіти: бакалавр, магістр, доктор філософії. Спеціалізація спрямована на опанування випускниками спеціальних знань із:

- проектування апаратів багатоканальних приймально-передавальних пристроїв, що працюють в середовищі з багатьма службами та технологіями одночасно;
- проектування програмно визначених засобів та систем телекомунікацій;
- розробки програмного забезпечення для пристроїв електронних комунікацій з урахуванням сучасних потреб у використанні функцій навігації, синтезу/аналізу сигналів, спеціалізованих методів обробки даних;
- розробки програмного забезпечення для вбудованих систем телекомунікацій (комутатори, мультиплексори, побутові приймачі цифрових сигналів, модеми і т.і.)
- розробки апаратно-програмних засобів розумних всепроникних мереж.

Рівень бакалавра забезпечує надбання випускниками компетенцій стосовно теоретичних основ побудови, монтажу та налагодження, контролю і діагностування стану, профілактики і відновлювального техобслуговування апаратно-програмних засобів електронних комунікацій.

Рівень магістра забезпечує надбання компетенцій по вдосконаленню, проектуванню та створенню апаратно-програмних комплексів електронних комунікацій.

Рівень доктора філософії забезпечує надбання компетенцій по здійсненню наукових досліджень, пошукових робіт та прогнозуванню напрямків розвитку апаратно-програмних телекомунікаційних засобів, проектуванню та впровадженню прототипів апаратно-програмних комплексів електронних комунікацій наступних поколінь.

Література

1. Kravchuk S., Afanassieva L. Development of telecommunication technologies as a factor of modern economic system // Materials of International scientific and practical conf. “Economics, science, education: integration and synergy”, Bratislava, Slovak Republic, 18–21 January, 2016: in 3 vol. – Vol. 3. – Bratislava, 2016. – P. 97–98.

УДК 621.391

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ТЕНЗОРНОГО ПІДХОДУ ДЛЯ ОПИСУ ДИНАМІКИ ЗМІНИ СТАНУ МЕРЕЖІ ПРИ ЗАБЕЗПЕЧЕННІ ЯКОСТІ ОБСЛУГОВУВАННЯ

Лемешко О.В., Єременко О.С.
Харківський національний університет радіоелектроніки, Україна
E-mail: oleksandr.lemeshko@nure.ua, oleksandra.yeremenko@nure.ua

Specifics of using the tensor approach to representation of network state change dynamics with ensuring Quality of Service

Proposed and investigated dynamic tensor model of QoS-routing over multiple metrics based on geometrization and tensor generalization of differential equations of network state, which adequately describe network links utilization and average packet delays. Results of research demonstrated that the use of dynamic tensor model allows more precisely calculate the values of average packet delay, especially under high utilization of network interfaces.

Відмінною ознакою сучасних телекомунікаційних мереж (ТКМ) є висока динамічність процесів інформаційного обміну. Стан мережі (завантаженість її інтерфейсів, затримки пакетів) змінюється в реальному масштабі часу: за десятки – сотні мілісекунд. Тому перспективні протоколи та механізм управління трафіком повинні ґрунтуватися виключно на динамічних моделях стану мережі. Перш за все це стосується моделей, які описують процеси маршрутизації та управління чергами на мережних інтерфейсах. В зв'язку з цим пропонується динамічна тензорна модель ТКМ, що описує процес багато шляхової маршрутизації із забезпеченням якості обслуговування одночасно за множиною показників QoS.

В рамках моделі багатошляхової маршрутизації структура ТКМ описується однорозмірною мережею $S=(U,V)$, де $U=\{u_i, i=\overline{1,m}\}$ – множина вузлів мережі (маршрутизаторів), а $V=\{v_z=(i,j); z=\overline{1,n}; i,j=\overline{1,m}; i\neq j\}$ – множина дуг (каналів зв'язку). При цьому дуга $v_z=(i,j)\in V$ моделює z-й канал зв'язку (КЗ), що з'єднує i-й і j-й маршрутизатори. Вважається, що пропускна здатність $\varphi_{(i,j)}$ відома для кожного каналу (i,j) і вимірюється в пакетах за секунду (1/с).

Результатом розв'язання задачі маршрутизації буде розрахунок множини маршрутних змінних $x_{(i,j)}^{k_p}$, кожна з яких характеризує частку інтенсивності k-го потоку p-го класу ($p=\overline{1,P}$, $k_p\in K_p$, $K_p\in K$, де K – множина потоків в мережі, а K_p – множина потоків p-го класу) від i-го вузла до j-го вузла через відповідний j-й інтерфейс.

З метою запобігання перевантаженню в кожному з вузлів і ТКМ в цілому необхідно виконання умови збереження потоку для вузлів відправник та отримувач, а також транзитних вузлів, відповідно, що може бути представлено у вигляді [1]:

$$\begin{cases} \sum\limits_{j:(i,j)\in V} x_{(i,j)}^{k_p} = 1,\ k_p \in K_p,\ i = s_{k_p}; \\ \sum\limits_{j:(i,j)\in V} x_{(i,j)}^{k_p} - \sum\limits_{j:(j,i)\in V} x_{(j,i)}^{k_p} = 0,\ k_p \in K_p,\ i \neq s_{k_p}, d_{k_p}; \\ \sum\limits_{j:(j,i)\in V} x_{(j,i)}^{k_p} = -1,\ k_p \in K_p,\ i = d_{k_p}, \end{cases} \quad (1)$$

де s_{k_p} – вузол відправник, а d_{k_p} – вузол отримувач для k-го потоку p-го класу.

Для реалізації стратегії багатошляхової маршрутизації з балансуванням навантаження на керуючі (маршрутні) змінні накладаються наступні обмеження

$$0 \le x_{(i,j)}^{k_p} \le 1. \quad (2)$$

Передумовою для керованості процесу маршрутизації є запобігання перевантаження КЗ за пропускною здатністю, тобто умова $\rho < 1$ (де $\rho = \lambda / \varphi$ – завантаженість КЗ):

$$\sum_{k_p \in K_p} \lambda_{req}^{k_p} x_{(i,j)}^{k_p} \le y_{(i,j)}^{p} \varphi_{(i,j)},\ (i,j) \in E, \quad (3)$$

де $\lambda_{req}^{k_p}$ – середня інтенсивність k-го потоку p-го класу, що надходить до мережі; $y_{(i,j)}^{p}$ – керуюча змінна, яка характеризує частку пропускної здатності $\varphi_{(i,j)}$, що виділяється для потоків p-го класу ($0 \le y_{(i,j)}^{p} \le 1$). Це значення є необхідною швидкістю передачі пакетів – однією з метрик QoS.

У ході розв'язанні наведеної маршрутної задачі мінімізується цільова функція наступного вигляду:

$$J = \sum_{(i,j)\in E} \sum_{p\in P} \sum_{k_p \in K_p} h_{(i,j)}^{x_p} \cdot x_{(i,j)}^{x_p} + \sum_{(i,j)\in E} \sum_{p\in P} h_{(i,j)}^{y_p} \cdot y_{(i,j)}^{p}, \quad (4)$$

де $h_{(i,j)}^{x_p}$ – маршрутна метрика каналу зв'язку між i-м та j-м вузлами ТКМ; $h_{(i,j)}^{y_p}$ – метрика розподілу пропускної здатності за потоками різних класів.

З метою отримання тензорної моделі ТКМ була представлена анізотропною просторовою структурою, утвореною множиною контурів і вузлових пар. Розмірність цього простору визначається загальною кількістю КЗ в мережі. В рамках тензорного узагальнення в якості моделі динаміки змін стану інтерфейсу маршрутизатора ТКМ була обрана математична модель, заснована на використанні системи нелінійних диференційних рівнянь стану мережі, отриманих за допомогою стаціонарної потокової точкової апроксимації (Pointwise Stationary Fluid Flow Approximation, PSFFA) [2]. Згідно цієї апроксимації середня затримка пакетів на інтерфейсі маршрутизатора змінюється наступним чином:

$$\frac{d\tau_{(i,j)}^{p}(t)}{dt} = 1 - \varphi_{(i,j)}^{p} \left(\frac{\tau_{(i,j)}^{p}(t)}{\lambda_{(i,j)}^{p} \tau_{(i,j)}^{p}(t) + 1} \right), \quad (5)$$

де $\varphi_{(i,j)}^{p} = y_{(i,j)}^{p} \varphi_{(i,j)}$ – пропускна здатність каналу (i,j), що виділяється для

потоків p-го класу; $\lambda^{p}_{(i,j)} = \sum_{k_p \in K_p} \lambda^{k_p}_{req} \cdot x^{x_p}_{(i,j)}$ – сумарна інтенсивність потоків p-го класу в каналі (i, j).

В результаті геометризації структури ТКМ, ґрунтуючись на тензорному узагальненні виразу (5), тензорна метрика стала функцією часу та для кожного КЗ має наступний вигляд:

$$g^{ij}_{v}(t) = \lambda^{i}_{v}(\varphi - \lambda) \cdot [(\varphi \cdot W(0, -(\lambda \cdot \exp(-(\lambda + (t - \\ -(\lambda + \varphi \cdot \ln(\exp(-(\lambda \cdot (\tau_0 \lambda - \tau_0 \varphi + 1))/\varphi) \cdot \\ \cdot (\tau_0 \lambda - \tau_0 \varphi + 1)))/(\varphi - \lambda)^2) \cdot (\varphi - \lambda)^2)/\varphi))/\varphi))/\lambda + 1]^{-1}, \quad (6)$$

де $W(\cdot)$ – W-функція Ламберта; $\exp(\cdot)$ – експоненціальна функція; τ_0 – середня затримка на інтерфейсі маршрутизатора в початковий момент часу.

Тоді в рамках тензорної моделі при розв'язанні задачі забезпечення QoS в ТКМ при заданих кількісних вимогах щодо середньої затримки та швидкості передачі пакета аналітичні умови забезпечення QoS наступні:

$$\lambda^{req} \le \left(G^{\langle 4,1 \rangle}_{\pi\eta}(t) - G^{\langle 4,2 \rangle}_{\pi\eta}(t) \left[G^{\langle 4,4 \rangle}_{\pi\eta}(t) \right]^{-1} G^{\langle 4,3 \rangle}_{\pi\eta}(t) \right) \tau_{req}, \quad (7)$$

де форма та зміст матриць $G^{\langle \dots \rangle}_{\pi\eta}(t)$ залежать від структури мережі, пропускних здатностей КЗ та дисциплін обслуговування пакетів [3, 4].

Результати дослідження запропонованої динамічної тензорної моделі показали, що за її допомогою вдалося більш точно розрахувати значення середньої затримки пакетів, особливо в умовах високої завантаженості інтерфейсів мережі. Так, наприклад, при завантаженості інтерфейсів ρ =0,63...0,82 похибка складала від 15% до 40%, що на практиці супроводжується, як правило, неефективним перерозподілом мережного (канального та буферного) ресурсу між потоками різних класів.

Література

1. Lemeshko A.V., Evseeva O.Yu., Garkusha S.V. Research on Tensor Model of Multipath Routing in Telecommunication Network with Support of Service Quality by Greate Number of Indices // Telecommunications and RadioEngineering, 2014, Vol.73, No 15. - P. 1339-1360.
2. Wei-Ping Wang, David Tipper, Sujata Banerjee. A Simple Approximation for modeling Nonstationary Queues // Proceedings of the Fifteenth Annual Joint Conference of the IEEE Computer Societies (INFOCOM '96). – 1996. – V.1. – P. 255–262.
3. Olexandr V. Lemeshko, Sergey V. Garkusha, Oleksandra S. Yeremenko, Ahmad M. Hailan Policy-based QoS Management Model for Multiservice Networks / O.V. Lemeshko, S.V. Garkusha, O.S. Yeremenko, A.M. Hailan // 2015 International Siberian Conference on Control and Communications (SIBCON). Proceedings. – Omsk: Omsk State Technical University. Russia, Omsk, May 21−23, 2015. – PP. 1–4.
4. Lemeshko O., Yeremenko O. Dynamic presentation of tensor model for multipath QoS-routing // Modern Problems of Radio Engineering, Telecommunications and Computer Science. Proceedings of the international Conference TCSET'2016. – Lviv-Slavsko, Ukraine, February 23 - 26, 2016: Publishing House of Lviv Polytechnic, 2016. – PP. 601-604.

УДК 621.396

РОЗРОБКА ТА ДОСЛІДЖЕННЯ ІМІТАЦІЙНОЇ МОДЕЛІ БЕЗПРОВІДНОЇ ГЕТЕРОГЕННОЇ МЕРЕЖІ

Климаш М.М., Масюк А.Р., Бешлей М.І.
Інститут телекомунікацій, радіоелектроніки та електронної техніки
Національний університет «Львівська політехніка», Україна
E-mail: mklimash@polynet.lviv.ua, beshlebmi@gmail.com

Research and development of simulation model for wireless heterogeneous networks

In this paper we have proposed the simulation model for mobile heterogeneous networks using OPNET modeler. Integration scenarios networks LTE, UMTS with Wi-Fi technology, taking into account the mobility of subscribers and the type of services have been considered.

Різноманітність технологій радіодоступу і збільшення кількості мультистандартних абонентських пристроїв дають змогу інтегрувати різноманітні технології в єдину мережу, тобто сформувати гетерогенну (неоднорідну) безпровідну мережу. Така мережа буде складатися з сегментів різних технологій радіодоступу, зони покриття яких накладаються. Це дасть змогу збільшити пропускну здатність мережі та розширити зону її покриття, а для мобільних пристроїв надавати зв'язок за нижчою ціною і з високою якістю обслуговування. Основна мета роботи полягає в наданні мобільному пристрою ефективного та безперервного обслуговування в гетерогенних безпровідних мережах, виходячи з вимог виконання функцій мобільних пристроїв та розвитку оптимальних алгоритмів ініціації вертикального хендовера. Для досягнення даної розроблено імітаційну модель гетерогенної мережі доступу в програмному середовищі OPNET MODELER 15(Рис.1) . Задачею моделювання є дослідження процесу інтеграції Wi-Fi/LTE та Wi-Fi/UMTS з ініціацією вертикального хендовера та оцінка виграшу при балансуванні навантаження.

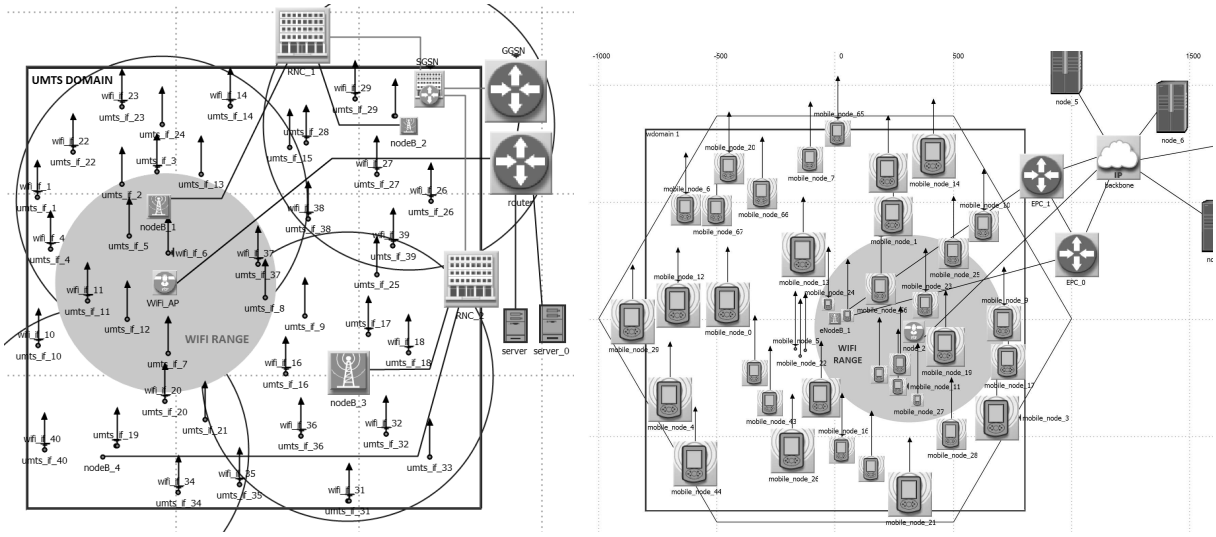


Рис. 1. Модель інтеграції технологій Wi-Fi/UMTS та Wi-Fi/LTE.

Однією з часто використовуваних моделей при моделюванні мобільних

мереж є модель випадкової точки маршруту, в якій вузли рухаються незалежно до випадково обраної цілі з випадково обраною швидкістю.

Простота даної моделі стала однією з причин її широкого застосування в моделюванні. Моделі мобільності можуть мати різні властивості і володіти різними характеристиками. Тому, щоб ретельно оцінити можливість виникнення перевантаження, необхідно використовувати багатий набір моделей мобільності та параметрів мережі замість моделі випадкової точки маршруту, які є добре реалізовані в середовищі Opnet Modeler (рис. 2).

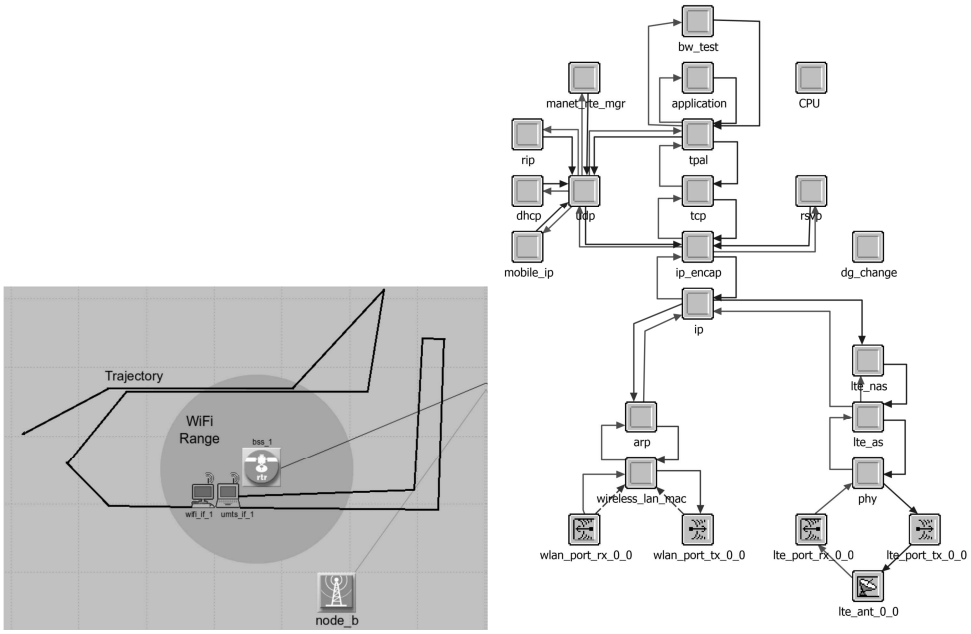


Рис. 2. Мобільність абонента та стек протоколів вузла з інтерфейсами Wi-Fi/LTE

Першим етапом дослідження є інтеграція UMTS\Wi-Fi мережі. У цьому випадку, кількість абонентів, які моделюються в мережі становить 40 терміналів. Абоненти довільно рухаються по зображеній площині квадрата в залежності від моделі мобільності RandomWaypoint [1] зі швидкістю, яка рівномірно розподілена в інтервалі між 0 і 5 м / с. Якщо абонент встановив активне з'єднання через систему UMTS і, не перериваючи його, увійшов в зону покриття не ліцензованої бездротової мережі Wi-Fi, поточне з'єднання автоматично перемикається на іншу мережу без переривання послуги. Рівень сигналу покриття Wi-Fi зони, становить 7 дБм (приблизно 5 мВт). Кожен мобільний термінал намагається кожної секунди завантажити файл розміром 30 кбайт, в результаті загальне навантаження від 40 абонентів становить 1200 Кб/с. Кількість базових станцій UMTS мережі становить 4, щоб забезпечити UMTS з'єднання для всіх мобільних терміналів у виділеній площині квадрата, позначеної як "UMTS ОБЛАСТЬ". На рисунку 3, показано відповідну кількість підключених мобільних терміналів та загальне навантаження на мережу протягом часу моделювання. В результаті моделювання встановлено, що загальне навантаження є зростаючою функцією часу. Це пов'язано з тим, що кількість активних терміналів в мережі постійно збільшується і, отже, загальний отриманий трафік на кожному інтерфейсі стає більшим. Крім того,

з рисунку 3, можна побачити, що, коли обидва інтерфейси мобільного пристрою є активні, загальне навантаження становить 1000 кб / с, що є наближеним до максимального можливого значення 1200 кб / с. З іншого боку, коли активний тільки інтерфейс UMTS , трафік становить приблизно 800 кб / с. Таким чином, наявність зв'язку Wi-Fi забезпечує додатковий зв'язок, необхідний для досягнення (теоретично) максимально можливого завантаження та балансування навантаження.

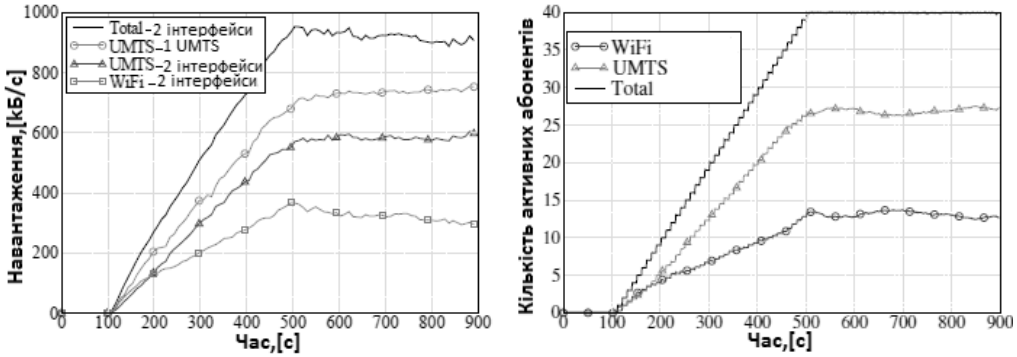


Рис. 3. Кількість підключених мобільних терміналів та загальне навантаження на мережу UMTS\Wi-Fi

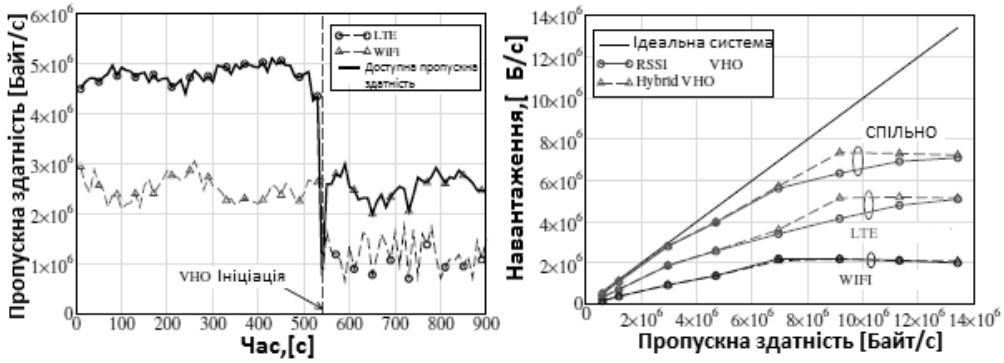


Рис. 4. Необхідна пропускна здатність для надання сервісу з ініціацією VHO (вертикального хендовера) в інтегрованій LTE/Wi-Fi мережі

На рисунку 4, представлено сценарій моделювання роботи інтегрованої LTE/Wi-Fi мережі в якій зареєстровано 40 абонентів, що рухаються по площині чотирикутника. Модель мобільності і швидкості руху користувачів такі ж, як і у попередньому сценарії.

В процесі моделювання встановлено, що при передаванні трафіку через мережу LTE в момент недостатності ресурсів для його обслуговування відбувається процедура вертикального хендовера і необхідні ресурси для даного сервісу забезпечує Wi-Fi мережа.

Висновки. Розроблена гетерогенна мережа є набагато ефективнішою в наданні сервісів абонентам, оскільки дозволяє балансувати навантаження між двома системами доступу.

Література

1. M. Klymash, M. Seliuchenko, M. Beshley, M. Brych. Mobility Management and Vertical Handover Decision in an Always Best Connected Heterogeneous Network. Proceedings of international conference CADSM'2015. Polyana-Svalyava. – 2015. p. 103-105.

УДК 528.831.1

ПІДВИЩЕННЯ ІНФОРМАТИВНОСТІ ЗОБРАЖЕНЬ ДАЛЬНЬОГО ІНФРАЧЕРВОНОГО ДІАПАЗОНУ НА ОСНОВІ СУБПІКСЕЛЬНОЇ ОБРОБКИ

Станкевич С.А., Шкляр С.В., Подорван В.М., Лубський М.С.
Науковий центр аерокосмічних досліджень Землі ІГН НАН України
E-mail: nickolo1990@gmail.com

Thermal infrared imagery enhancement using sub-pixel processing

Spatial resolution is the main specification of infrared imagery quality. Many technical restrictions do not allow realizing the high spatial resolution of thermal infrared band imagers. The software-based method for infrared imagery spatial resolution enhancement is presented. The method used two sub-pixel shifted images that contain time-invariant thermal emissivity data. Enhanced spatial resolution infrared imagery provides better informativity for remote sensing application.

Здатність сенсорних систем формувати зображення високої просторової розрізненності знижується разом із підвищенням довжини хвиль, на чутливість до яких орієнтується дана система. Це пов’язано із рядом фізичних обмежень, таких як зниження енергії квантів світла та необхідність підвищення лінійних розмірів детекторних елементів [1].

Таким чином, для підвищення просторої розрізненності доцільно застосовувати програмні методи. Одним із таких методів є застосування кількох субпіксельно зміщених одне відносно одного зображень.

Часто даний метод застосовуються для підвищення просторової розрізненності проміжних даних для підвищення якості результатів обробки зображень у тепловому інфрачервоному діапазоні, одним із найбільш поширених джерел яких є сенсор TIRS на борту супутника Landsat-8, із просторовою розрізненністю 100 м. Дані цього сенсора є основою для точного визначення температури різноманітних природних та штучних поверхонь [2], що дозволяє вирішити широкий спектр задач.

Субпіксельно зміщені зображення, для яких застосовується підвищення просторової розрізненності мають містити інваріантні дані із мінімальними розбіжностями. У випадку із обробкою даних теплового знімання найбільш доцільно застосовувати два зображення коефіцієнтів теплового випромінювання для досліджуваної території, отримані із мінімально можливим часовим інтервалом. Коефіцієнт теплового випромінювання – власна характеристика поверхні, яка описує її здатність поглинати тепло та дозволяє визначати фізичну температуру поверхні за даними дистанційного теплового знімання. При цьому за період повторного проходження над дослідною територією супутника (16 днів) зміни коефіцієнтів теплового випромінювання більшості об’єктів сцени є мінімальними а для деяких об’єктів (штучні поверхні, водні об’єкти) є незмінним.

Першим етапом підвищення просторової розрізненності є оцінка

субпіксельного зміщення одного зображення відносно іншого, за допомогою опорних текстур із чіткими контурами та високим контрастом відносно інших частин зображення, в результаті якої отримуються значення та напрям зміщення по горизонтальній та вертикальній осях.

Наступний етап – відновлення зображень підвищеної розрізненності у субпікселах $x_{ij}\, i = 1 .. n_x+p-1,\ j = 1 .. n_y+q-1$ по відомих значеннях зображення y_{ij} в пікселах вхідного набору зображень низької розрізненності, зміщених на $^1/_p$ та $^1/_q$ частки піксела вздовж осей x та y відповідно. Значення пікселів виражаються через субпіксельні зміщення системою рівнянь:

$$y_{ij} = \sum_{k=1}^{i+p-1} \sum_{l=1}^{j+q-1} x_{kl} \ , \quad i = 1 .. n_x \ , \quad j = 1 .. n_y \ . \tag{1}$$

яка складається з $n_x \times n_y$ рівнянь з $(n_x+p-1)\times(n_y+q-1)$ невідомими. Строгий розв'язок системи (1) знаходиться за рекурентною формулою:

$$x_{ij} = y_{(i-p+1)(j-q+1)} - \sum_{k=i-p+1}^{i-1} \sum_{l=j-q+1}^{j-1} x_{kl} - \sum_{k=i-p+1}^{i-1} x_{kj} - \sum_{l=j-q+1}^{j-1} x_{il} \ , \ i = p .. n_x+p-1,$$

$$j = q .. n_y+q-1. \tag{2}$$

Щоб запобігти накопиченню шумів, можна застосовувати розв'язок у прямокутному вікні зображення. Для розв'язку застосовується вікно розмірністю $w \times u$ пікселів низької розрізненності для оцінювання єдиного піксела підвищеної розрізненності x_{ij}. Припускаючи, що $w+p-1$ та $u+q-1$ є непарними числами, розв'язок x_{ij} з мінімальною вибірковою дисперсією при $(w+p-1)\times(u+q-1)$ невідомих може бути знайдено із системи рівнянь:

$$y_{ij} = \sum_{k=i}^{i+p-1} \sum_{l=j}^{j+q-1} x_{kl} \ , \ k = i-{}^{(w+p)}/_2-1 .. i+{}^{(w-p)}/_2 \ , \ l = j-{}^{(u+q)}/_2-1 .. j+{}^{(u-q)}/_2 \ . \tag{3}$$

Модель відновлення зображення підвищеної просторової розрізненності із включеними шумами можна виразити наступним чином:

$$X = R \times Y + \varepsilon \ , \tag{4}$$

де X – зображення підвищеної розрізненності, розгорнуте у вектор, Y – ряд зображень низької розрізненності, розгорнутих у вектори, R – матриця оператора пересемплювання, ε – вектор похибок [3].

Приклад відновлення зображень підвищеної розрізненності за допомогою субпіксельного зміщення представлено на рис. 1.

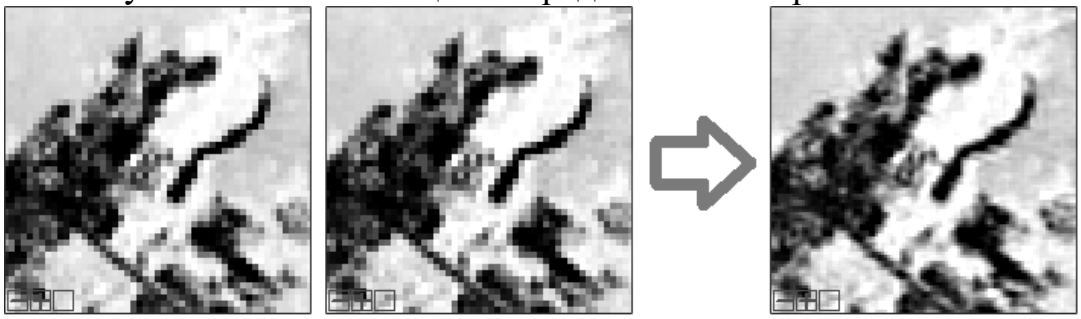
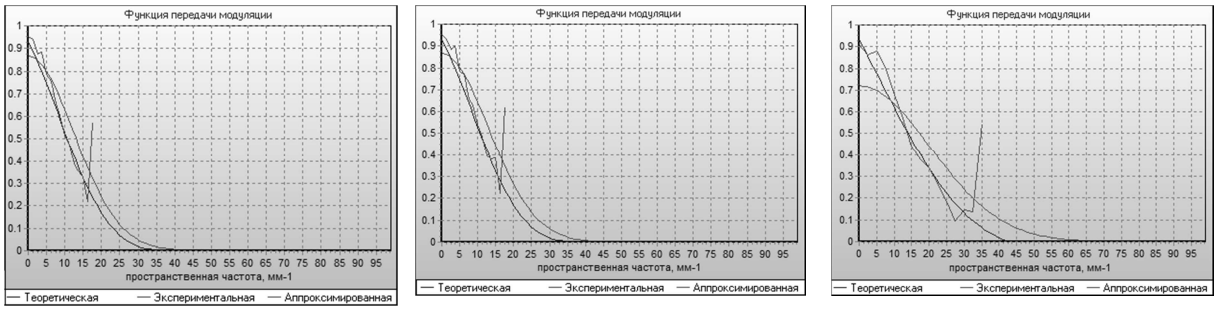


Рис. 1. Відновлення зображення підвищеної розрізненності.

Оцінка підвищення якості виконується на основі розрахунку функції передачі модуляції вихідних зображень та результуючого зображення. В оцінку окрім самих зображень включаються параметри польоту знімальної системи: висота знімання (висота орбіти Landsat-8 становить 705 км) та швидкість носія – 7,9 км/с, та параметри сенсорної системи: фокусна відстань оптики – 17,8 мм, час експонування – 7,5 мкс, відносний отвір оптики– 0,61, половина кута огляду – 7,475 градусів та розмір фотоприймального елементу 25 мкм [4]. Для результуючого зображення розмір елементу вказується вдвічі меншим.

Результати оцінки представлено на рис. 2.



а *б* *в*

Рис. 2. Функції передавання модуляції зображень.

а, б – вхідних зображень, *в* – результуючого після субпіксельної обробки вихідних зображень

Значення ФПМ на рівні 0,3 відповідають розрізненності 15 $мм^{-1}$ для зображення рис. 2*а*, 16 $мм^{-1}$ – для зображення рис. 2*б* і 22 $мм^{-1}$ – для зображення рис. 2*в*. Таким чином, підвищення просторової розрізненності складає 46 %.

В подальшому покращене зображення коефіцієнтів теплового випромінювання застосовується для отримання карт температур на основі даних супутникового теплового знімання, наприклад, зображень сенсора TIRS.

Література

1. Neumann K.J. Trends for digital aerial mapping cameras // The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, 2008.– Vol.XXXVII.– Part B1.– P.551-554.
2. Станкевич С.А. Оцінка точності визначення температури штучних та природних земних поверхонь за результатами інфрачервоного космічного знімання / Станкевич С.А., Пилипчук В. В., Лубський М.С., Крилова Г.Б. // Космічна наука і технологія,– 2016, [У друці].
3. Станкевич С.А. Підвищення просторової розрізненності аерознімання на основі субпіксельної реєстрації зображень / С.А. Станкевич, С.В. Шкляр, М.С. Лубський // Збірник наукових праць Державного науково-дослідного інституту авіації.– Вип.9(16).– Київ: ДНДІА, 2013.– С.110-117.
4. Reuter, D. C., C. Richardson, J. Irons, et al. 2010. "The Thermal Infrared Sensor on the Landsat Data Continuity Mission." IEEE International Geoscience Remote Sensing Symposium 754-757.

УДК 621.396

ЦІЛЬОВІ ФУНКЦІЇ УПРАВЛІННЯ ПОВІТРЯНОЮ РАДІОМЕРЕЖЕЮ

Романюк В.А.
Військовий інститут телекомунікацій та інформатизації, Україна
E-mail: rom-v-a@yandex.ua

Objective control functions of flying ad-hoc networks

A new approach to the selection of objective control functions of VANET using UAV, based on the current control functions formation, depending on the traffic type, current situation in the network and available network resources.

Повітряна радіомережа (ПР) представляє собою мережу типу VANET та складається з множини безпілотних літальних апаратах або повітряних телекомунікаційних аероплатформ (ТА) та призначена для: забезпечення заданих показників якості обслуговування мобільних абонентів; встановлення зв'язності в мережі з географічно віддаленими абонентами (зонами мережі); збору інформації від сенсорних мереж (полів, окремих сенсорів); моніторингу заражених районів, цілях про противника тощо [1 – 3]. До основних особливостей функціонування ПР можна віднести: значну динаміку зміни її топології, різнорідний трафік, колективне використання радіоресурсу, нестабільність радіоканалів та наявність взаємних перешкод, обмеженість та неоднорідність ресурсів вузлів, обмежену безпеку через широкомовну природу радіоканалу, високу ймовірність радіоелектронної протидії супротивника та ін.

Наземні (сенсори, мобільні абоненти, мобільні базові станції) та повітряні вузли мережі повинні швидко адаптуватися до частих змін топології мережі, трафіка та ефективно використовувати обмежені мережеві ресурси. В таких умовах забезпечити інформаційний обмін з заданою якістю неможливо без ефективної системи управління мережею [2], яка повинна відповідати наступним вимогам: адаптивність, функціональність, координація взаємодії, децентралізоване управління тощо.

Управляючі впливи системою управління мережею здійснюються на основі реалізації циклу управління: збору та аналізу інформації про стан мережі, ідентифікації ситуації про стан мережі та прийняття управляючого рішення по забезпеченню якості передачі трафіка. В процесі прийняття рішення виникає завдання щодо визначення цільових функцій управління мережею або її зоною.

Раніш запропоновані підходи пропонували здійснювати оптимізацію визначених мереж за одним або декілька показниками [3 – 6]. Так в [3] запропоновано управляти витратами енергії батарей, в [5] здійснювати багатокритеріальну оптимізацію маршруту с врахуванням його мобільності, в [6] оптимізувати топологію мережі за декількома показниками тощо.

Пропонується новий підхід – на етапі управління мережею цільові функції управління не є статичними, а визначаються в часі в залежності від

етапів и функцій управління, а також параметрів стану об’єкта (об’єктів) управління (вузол, радіоканал, маршрут, зона, мережа) та наявних ресурсів [7].

Визначимо особливості задач управління ПР (рис. 1): реалізуються на різних етапах управління мережею; мають окремі функціональні призначення; різні об’єкти впливу; різні цільові функції, можуть заперечувати одна одної; різняться математичною постановкою цільових функцій; мають високу розмірність та динамічний характер; важкість формування повної системи показників оцінки ефективності; неповнота та часто недостовірність контрольної інформації про стан мережі та її елементів; більшість з них залежать друг від друга; вимагають узгодження та координації (в вузлах, маршрутах, зонах, в масштабах всієї мережі); можуть бути реалізовані на різних рівнях еталонної моделі OSI.

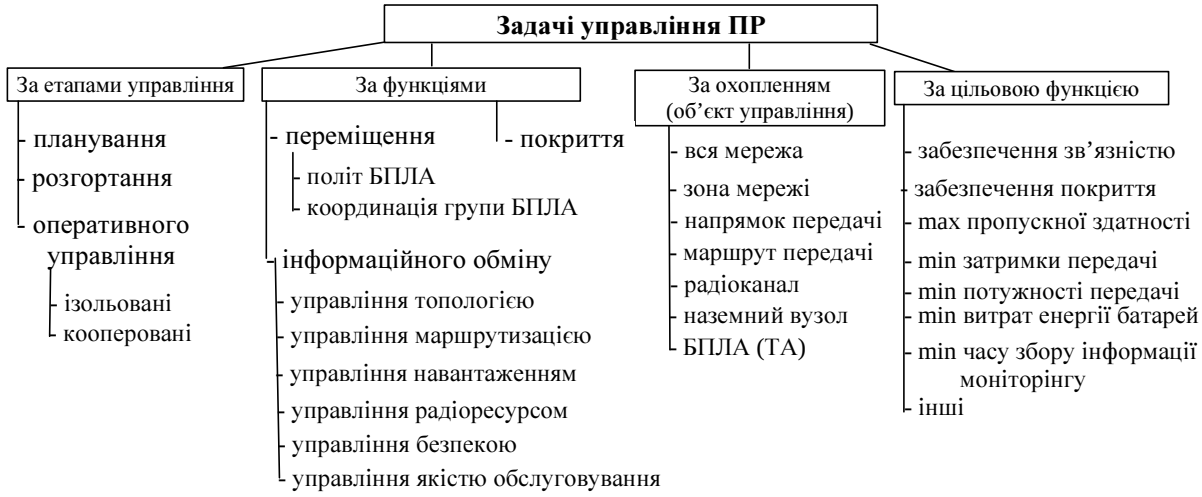


Рис. 1. Класифікація задач управління повітряною радіомережею.

В умовах змішаного управління (частка функцій виконується централізовано центрами управління, а друга децентралізовано – вузлами) можна визначити дві взаємозалежні групи цілей:

мережеві (зонові) – оптимізація мережевих або зонових показників ефективності;

користувальницькі – досягнення заданої якості передачі між абонентами та функціонування елементів мережі за напрямком передачі.

До мережевих (зонових) цілей управління можна віднести оптимум наступних параметрів $C_i = \{C_1, C_2, \ldots, C_n\}$:

C_1 – продуктивність всієї мережі, зони, ПР;

C_2 – потужність передач вузлів мережі, її зони;

C_3 – ступінь покриття території (абонентів, сенсорів) повітряною мережею;

C_4 – структурна надійність (зв'язність) мережі, її зони;

C_5 – кількість ресурсів (вузлів, мобільних базових станцій, аероплатформ тощо), які необхідно задіяти до досягнення певної мети;

C_6 – час функціонування мережі, її зони, безпосередньо БПЛА (ТА);

C_7 – обсяг службового трафіка;

C_8 – час планування, розгортання, відновлення мережі, її зони;

C_9 – параметри безпеки й т.д.

Основними обмеженнями при цьому є ресурси и параметри вузлів: батареї живлення, пропускна здатність радіоканалів, дальність радіозв'язку, об'єми пам'яті, швидкість обробки інформації, параметри самої ТА тощо.

До основних користувальницьких цілей управління можна віднести оптимум (обмеження) наступних параметрів: пропускна здатність, час затримки передачі повідомлень, потужність передавача, енергія (витрати енергії) батарей в радіоканалі, маршруті, напрямку тощо.

В табл. 1 наведено об'єкти управління та основні параметри оптимізації. Наявність інформації, необхідної для передачі, вимагає систему управління кожного вузла здійснити вибір цілей (цільових функцій) управління, які повинні врахувати стан вузла, мережі, тип трафіка та наявні ресурси.

1. Стан самого вузла безпосередньо визначається множиною його параметрів: реальна пропускна здатність радіоканалів, дальність радіозв'язку, наявність сусідів, стан черг, наявність, тип та величина зміни вхідного навантаження, мобільність, динамка зміни наявних зв'язків з сусідами, наявність, кількість та якість побудованих маршрутів, тощо. Ресурсами вузла є апаратні (потенційна пропускна здатність радіоканалу, наявний обсяг енергії батареї живлення, швидкодія процесорів, потужність передавача тощо), програмні ресурси (алгоритми управління, протоколи управління на різних рівнях OSI та функціональних підсистемах, рівень інтелектуалізації процесів управління тощо).

Кожен вузол постійно (активно або/та пасивно) збирає інформацію про стан: вузлів-сусідів, маршрутах та напрямах передачі, мережі (зони) та по сукупності показників визначає (ідентифікує) її стан [2].

2. Стан мережі (визначається станом вузлів, каналів, напрямків, зони та всієї мережі, наявністю ресурсів) та динаміку його зміни.

3. Тип інформації (трафіка), який визначає вимоги до якості передачі (час передачі и джиттер, кількість помилок тощо).

Узагальнений алгоритм визначення цільових функцій управління системою управління кожного вузла наступний.

Вузол постійно аналізує свій стан та здійснює його ідентифікацію. Також вузол постійно збирає інформацію про стан мережі та здійснює ідентифікацію стану мережі (її зони). В умовах неможливості збору всієї інформації про стан мережі та її швидкого старіння системі (тобто неповної інформації про стан мереж)і для здійснення процесу ідентифікації пропонується використовувати апарат нечіткої логіки [2].

Система прийняття рішення вузла на основі ідентифікованих станів вузла, мережі та вимог до якості інформаційного обміну відносно інформації, яку має вузол на передачу (рис. 2):

- визначає поточну множини параметрів оптимізації – мережевих та користувальницьких;

- визначає об'єкти управління (табл. 1);

- визначає поточну цільову функцію (функції) управління – $optC_i$;

- узгоджує її зі вузлами-сусідами (якщо вузлі одного рангу) або нав'язує її підпорядкованим вузлам (якщо це центр управління мережею);

- вибирає управляючій вплив за етапами, охопленням, функціональною підсистемою, рівнем OSI.

Табл. 1

Рівень OSI	***Управляючий вплив вузла***	***Об'єкти управління***	***Основні параметрі оптимізації***
Фізичний	Потужність (спрямованість) передачі, вид модуляції, тип коригуючого коду, параметри MIMO тощо	Радіоканал: ТА-ТА, наземний вузол-наземний вузол, наземний вузол-ТА	Пропускна здатність, витрати енергії батарей, потужність передачі тощо
Канальний	MAC-алгоритми та їх параметри, розміри пакетів та квитанцій тощо	Радіоканали в межах радіозв'язності зони	Пропускна здатність та час передачі в каналі, витрати енергії батарей, обсяг службової інформації тощо
Мережевий	Алгоритми маршрутизації, алгоритми управління чергами, алгоритми управління навантаженням, алгоритми управління топологією	Один або декілька маршрутів передачі (відповідно зона мережі або вся мережа), топологія, черги тощо	Обсяг службової інформації, параметри маршруту (час побудови та існування, кількість, пропускна здатність, час доставки, витрати енергії батарей тощо), топологія
Транспортний	Алгоритми обміну транспортного рівня	Напрямок зв'язку	Параметри якості передачі даних в напрямку
Додатків	Алгоритми (протоколи) інформаційного обміну прикладного рівня, координація та інтелекту-алізація за рівнями OSI, зонам мережі, всієї мережі	Вузол, вузли-сусіди, зона мережі, вся мережа	Пропускна здатність, витрати енергії батарей, безпека передачі, час виконання завдання тощо

В [7] наведена взаємозалежність цілей, а також їх ієрархічний характер, проведена декомпозиція глобальної мети управління мережею по функціях, кожна з яких ділиться на завдання й реалізується по рівнях OSI. Мета – одержання вектора пріоритету елементів нижнього рівня ієрархії стосовно цілі – елементу першого рівня за допомогою методу аналізу ієрархій або методу згортки нечітких відносин.

Цільова структура (ЦС) управління мережею:

$$\text{ЦС} \rightarrow H = \{C_1, R_{1m_{(1)}}\{C_{21}, C_{22}, ..., C_{2m_{(2)}}\}, R_{2m_{(2)}}\{C_{31}, C_{32}, ..., C_{3m_{(3)}}\}, ..., R_{km_{(k)}}\{C_{k1}, C_{k2}, ..., C_{km_{(k)}}\}\},$$

де C_1 – основна ціль системи управління, $C_{im_{(i)}}$ – $m_{(i)}$-а підціль і-го рівня на цільовій структурі, i =1…k, R – множина відносин на підцілі структури. Запропонована побудова ієрархії процесу вибору альтернатив та порівняння рішень на кожному рівні ієрархії на основі нормалізації отриманих оцінок альтернатив (застосовуючи процедуру зважування методу аналізу ієрархій або метод згортки нечітких відносин).

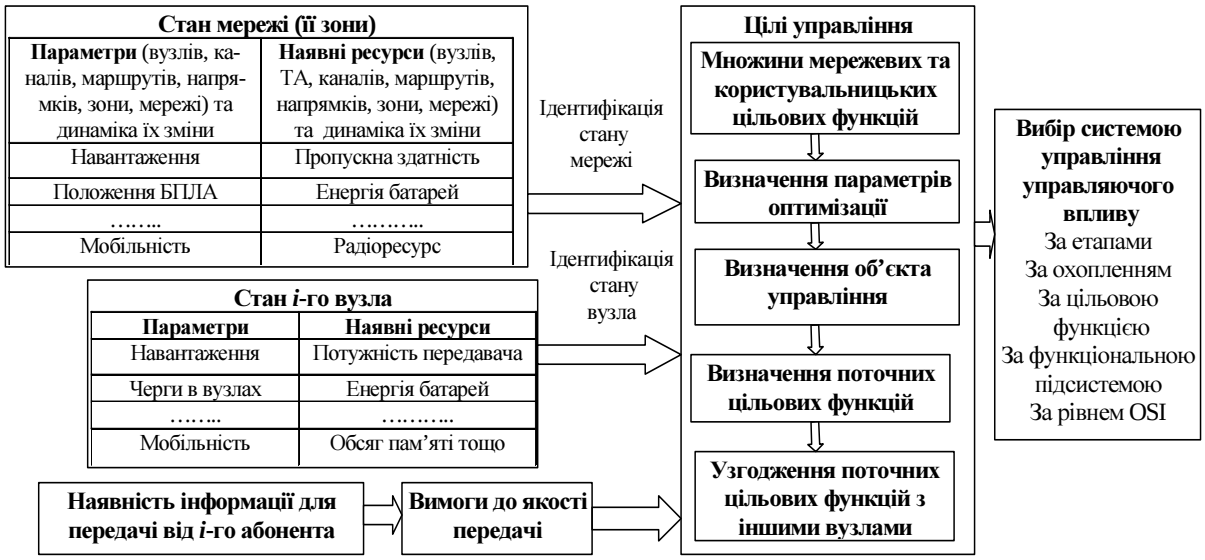


Рис. 2. Схема прийняття рішення системою управління ПР.

Завдання ухвалення рішення по управлінню мережею (вибір методів управління) зведена до завдання ієрархічного цільового динамічного оцінювання альтернатив при нечітких вихідних даних.

Таким чином проведена класифікація цільових функцій управлення повітряних радіомереж. Запропонований новий підхід до формування цільових функцій управління для цих мереж: кожен вузол визначає в часі поточну цільову функцію в залежності від типу трафіку, ситуації, що склалася на мережі та наявних мережевих ресурсів. Завдання прийняття рішення щодо вибору цільової функції управління радіомережі зведена до ієрархічного цільового оцінювання альтернатив. Запропонована схема формування цільових функцій управління може бути використана при побудові математичного забезпечення управління повітряною радіомережею.

Література

1. Bekmezci I., Sahingo O, Temel S. Flying Ad-Hoc Networks (FANETs): A survey // Ad Hoc Networks, 05/2013; 11(3):1254 – 1270.
2. Самоорганизующиеся радиосети со сверхширокополосными сигналами / [С.Г. Бунин, А.П. Войтер, М.Е. Ильченко, В.А. Романюк]. – К.: НПП „Издательство „Наукова думка" НАН Украины". – 444 с.: ил.
3. Gupta L., Jain R., Vaszkun G. Survey of Important Issues in UAV Communication Networks // IEEE Communications Survey and Tutorials, v. PP, Issue 99, November 2015.
4. Olascuaga-Cabrera J.G., Lopez-Mellado E., Mendez-Vazquez. A multi-objective PSO strategy for energy-efficient ad-hoc networking // IEEE Cybernetics Systems, Man (SMC) Conference, 2011.
5. Banner R., Orda A. Multi-Objective Topology Control in Wireless Networks // In Proc. IEEE INFOCOM, 2008.
6. Selvi R., Rajaram R. Muliple-objective optimization of multimedia packet scheduling for ad hoc networks through hybridized genetic algorithm // The International Journal of Multimedia & Its Applications (IJMA), Vol.3, No.3, August 2011.
7. Романюк В.А. Цільові функції оперативного управління тактичними радіомережами // Збірник наукових праць. – К.: ВІТІ НТУУ "КПІ". – 2012. – №1. – С. 109 – 117.

УДК 621.3

МЕТОДИКА РОЗРАХУНКУ ВИМУШЕНОГО РАМАНІВСЬКОГО РОЗСІЮВАННЯ В DWDM СИСТЕМІ

Орищук М.В., Романов О.І.
НТУУ «Київський політехнічний інститут», Україна
Email: maximshd@ukr.net, a_i_romanov@mail.ru

The method of calculation of stimulated Raman scattering in DWDM System

A large number of optical wavelength and huge amount of traffic create new non-linear process inside optical fiber. This paper dedicated on estimation stimulated Raman scattering (SRS) inside multi channel DWDM system. New integrated method of calculation was proposed. Practical estimation showed that SRS effect is mandatory for consideration in high-power multi channel system.

Ключові слова: нелінійні ефекти, оптичне волокно, вимушене Раманівське розсіювання, хвильове мультиплексування.

WDM технології набувають все більшої популярності при побудові магістральних ліній зв'язку. Найбільш привабливою особливістю даної технології являється можливість нарощування пропускної здатності без перебудови інфраструктори, а лише за рахунок введення нових хвиль. Тому, однією із найважливіших характеристик WDM системи являється кількість оптичних каналів, які можливо запустити в одному оптичному волокні. Так на провідне місце в останні роки вийшла DWDM система, яка дозволяє організувати до 80 оптичних каналів в одному фізичному, при цьому максимальна пропускна здатність такої системи може складати 6,4 Тбіт/с[2].

Незважаючи на всі переваги багатоканальної DWDM системи, вона має ряд обмежень, які при певних умовах значною мірою впливають на сигнал, який передається. Найбільш характерним і визначальним обмеженням, після затухання та дисперсії, являється міжканальна взаємодія. Можна виділити наступні перехресні перешкоди, викликані нелінійною взаємодією між світлом і матеріалом оптичного волокна: вимушене Раманівське розсіювання (SRS), вимушене Бріллюенівське розсіювання (SBS), фазова самомодуляція (SPM), перехрестна фазова модуляція (XPM) та чотирьох хвильове змішування (FWM).

Якщо в одноканальній оптичній системі вплив Раманівського розсіювання незначний, через малу потужність оптичного сигналу який передається, то в 80-канальній системі його вплив може в значній мірі вплинути на якість нашого сигналу в системі . Дана стаття присвячена впливу SRS на DWDM систему та визначенню основних енергетичних показників системи з SRS.

Вимушене Раманівське розсіювання виникає внаслідок взаємодії світла та молекулярної вібрації середовища розповсюдження (SiO_2). Як результат, відбувається перетворення частоти світлової хвилі. Дві нові спектральні компоненти з'являються навколо спектру корисного сигналу. Компонента з нижчою частотою називається хвилею Стокса і має набагато вищий рівень ніж компонента з вищою частотою. Це призводить до ослаблення енергії оптичного сигналу, що вводиться в волокно. Як правило, це не є проблемою для окремих

канальних систем, через відносно високий поріг потужності, при якому починається помітний вплив SRS на сигнал. Але якщо ми вводимо дві оптичні хвилі, які розташовані на відстані, що входить в смугу підсилення Стокса, в волокно, де присутня Раманівська взаємодія, потужність низьких частот буде збільшуватися за рахунок вищої частоти хвилі. Подібний обмін енергією між каналами називається перехрестною взаємодією. В більш складному випадку, коли кількість каналів N ≥ 2, низькі частоти підсилюються за рахунок більш високих лише у тому випадку, якщо різниця між їх частотами знаходиться в смузі раманівського підсилення[1].

Для оцінки SRS було сформовано ряд вхідних параметрів системи:

- Коефіцієнт ослаблення для кабелю G.652 α = 0.22 дБ/км,
- ефективна площа ядра A_{eff} = 36.33 мкм^2 ,
- довжина ділянки L = 100 км,
- довжина хвилі нульового каналу λ_0 = 1440 нм,
- раманівська смуга підсилення ΔF = 15 ТГц,
- рівень вхідного сигналу P_i = 600 мВ,
- кількість каналів в системі N = 8.

В якості топології DWDM мережі була взята топологія «точка-точка» без регенераційних секцій та проміжних підсилювачів (рис. 1).

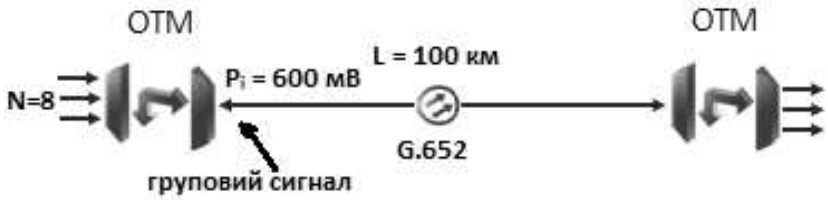


Рис. 1 Блок-діаграма досліджуваної схеми, де OTM – Optical Terminal Multiplexer.

Втрати потужності, які виникають в каналі через вплив SRS можуть бути обраховані як сума всіх потужностей, що передається до інших каналів на більш низьких частотах [1].

$$D = \sum_{i=1}^{N-1} \frac{f_0 * P_i * g_i * L_{eff}}{f_i * A_{eff}}, \quad (1)$$

де D – потужність сигналу, яке перерозподіляється по іншим частотам [Вт], i – номер каналу, f_0 – частота нульового каналу (канал із найбільшою частотою), f_i – частота i -го каналу, N – кількість каналів в DWDM системі, P_i – потужність на вході i-го каналу, L_{eff} – ефективна довжина оптичної лінії, A_{eff} – ефективна площа ядра оптичного волокна, g_i – раманівський коефіцієнт підсилення для i -го каналу.

Ефективна довжина лінії може бути виражена як[1]:

$$L_{eff} = \frac{1 - e^{-\alpha L}}{\alpha}, \quad (2)$$

де α – коефіцієнт загасання в оптичному волокні [дБ/км],

L – актуальна довжина оптичної лінії [км].

На другому етапі необхідно визначити рівень енергії, що виділиться на частоті Стокса. Ця енергія залежить від Раманівського коефіцієнта підсилення g_i, що в свою чергу залежить від різниці частот між каналами, які обмінюються енергією. Для G.652 коефіцієнт був знайдений експериментально. Було виявлено, що смуга Раманівського підсилення діє в смузі 40 ТГц [1](рис.2)

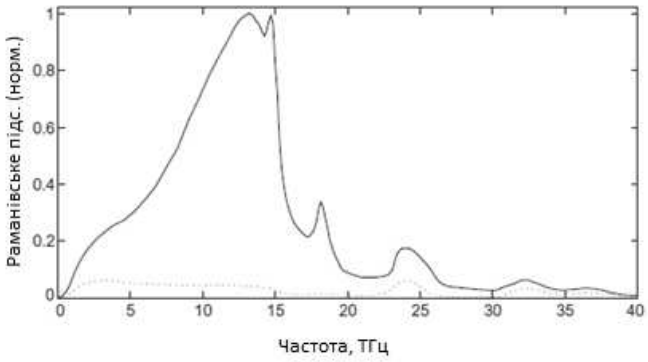


Рис. 2 Залежність нормованого коефіцієнта Раманівського підсилення від різниці між частотою накачки та частотою Стокса.

В спрощеному вигляді g_i можемо обрахувати за виразом[3]:

$$g_i = \frac{G\Delta f_{\text{i}}}{2\Delta F}, \quad (3)$$

Після визначення всіх необхідних показників, можемо розрахувати сумарну енергію що залишиться в цільовому каналі після дії SRS[3]:

$$P_{rem1} = -10\lg(1 - D), \quad (4)$$

Застосовуючи аналіз, запропонований в [4] отримуємо наступне рівняння для визначення частки потужності, що залишається в цільовому каналі (в дБ):

$$P_{rem2} = -10\lg(1 - \sum_{i=1}^{N-1} 1 - \exp(\frac{f_0 * P_i * g_i * L_{eff}}{f_i * A_{eff}})), \quad (5)$$

Результати дослідження SRS на основі запропонованої методики показали, що за достатньо високої потужності вхідного сигналу рівень втрат може складати значне значення. Так, для 8-канальної DWDM системи з вхідною потужністю сигналу 600 мВ, різниця між першим та останнім каналом сягає понад 8 дБ. При збільшенні кількості каналів в системі це значення буде сягати ще більшого значення. Таким чином, вимушене Раманівське розсіювання має значний вплив на оптичну систему передачі і його потрібно враховувати при проектування DWDM систем.

Література

1. G. P. Agrawal, Nonlinear Fiber Optics. Rochester, NY: Academic Press, 2013, 5th. ed. – 623.
2. ITU, Spectral grids for WDM applications: DWDM frequency grid, Recommendation ITU-T G.694.1, ser. Series G. International Telecommunication Union, 2012, 2nd ed.
3. S. P. Singh, R. Gangwar, and N. Singh, Nonlinear scattering effects in optical fibers. Progress In Electromagnetics Research, p. 379405, 2007.
4. ITU-T Study Group 15, Delayed Contribution D.170, Geneva, Feb. 9-20, 1998.

УДК 621.396.946

ПРИКЛАДНІ АСПЕКТИ ЗАСТОСУВАННЯ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ І БПЛА

Лисенко О.І., Валуйський С.В.
Інститут телекомунікаційних систем НТУУ «КПІ»
E-mail: samubf@gmail.com

Applied Aspects of Wireless Sensor Networks and UAVs

The article discusses new applied aspects of wireless sensor networks and UAVs, in particular remote data collection using UAV, drone application in telco for network optimization, tower audit and remote inspection, line of sight planning etc.

Безпроводові сенсорні мережі і безпілотні літальні апарати (БПЛА) на сьогодні знаходять широке коло застосування: моніторинг параметрів навколишнього середовища, моніторинг диких тварин і людської життєдіяльності, моніторинг надзвичайних ситуацій, трекінг цілей, доставка товарів і т. ін. Останнім часом зявляються спроби застосовувати БСМ і БПЛА навіть у телекому нікаціях. Зокрема компанією Nokia було проведено тестування дронів для оптимізації мережі мобільного оператора у місцях масового скупчення людей (стадіони, спортивні ігри тощо), віддаленої інспекції мобільних веж, планування лінії прямої видимості радіорелейних ліній зв'язку [1]. Разом із зростанням кількості дронів їх застосування виникають суміжні проблеми – безпека повітряного руху, віддалене управління і моніторинг польоту. Так компанією Nokia в рамках програми «Drones for good» було запропоновано систему моніторингу і управління польотами дронів із використанням LTE мережі [2]. Разом із ростом застосувань зростає і кількість наукових математичних задач, які потребують вирішення, зокрема планування оптимальної траєкторії польоту дронів, що мінімізує їх енерговитрати, чому і присвячена дана стаття.

При наявності групи БПЛА збір інформації з віддалених сенсорів можливо шляхом організації безпроводової сенсорної мережі із ретрансляцією (маршрутизацією) сигналів через мережу повітряних ретрансляторів, розташованих на БПЛА. Детально це розглядалося в [3]. Однак при цьому необхідною вимогою є повне радіо покриття сенсорів повітряними ретрансляторами (маршрутизаторами), що не завжди доцільно та не завжди вдається на практиці. Тому в даній роботі пропонується здійснювати збір інформації за допомогою одного БПЛА, що послідовно облітає всі сенсори, зчитує з них дані (коли знаходиться в зоні взаємної радіо видимості), запам'ятовує їх і «скидає» в пункт спостереження при поверненні в початкову точку. Це дасть змогу заощадити на кількості БПЛА, однак при цьому суттєво знизиться оперативність отримання інформації. Тому виникає необхідність пошуку такого маршруту польоту БПЛА, що дозволить

послідовно зчитати дані з усіх сенсорів та мінімізує сумарно пройдений шлях та відповідно паливні витрати БПЛА.

Здійснимо математичну постановку задачі. Нехай задано множину сенсорів $S = \{x_i, y_i\}, i = \overline{1,N}$, де N – кількість сенсорів, розміщених випадковим чином на площині (зоні спостереження) заданого розміру r з координатами (x_i, y_i). Нехай БПЛА переміщується у просторі на постійній висоті h з постійною швидкістю v по деякому маршруту M, що характеризується множиною опорних точок простору з координатами проекції на земну поверхню $\{x_j, y_j\}, j = \overline{1,K}$, де K – кількість точок в маршруті. Вважатимемо, що між точками маршруту БПЛА переміщується по прямолінійній траєкторії, а перша і остання точки співпадають та мають координати (0,0). Нехай БПЛА утворює на земній поверхні зону стабільного радіо покриття радіусу R. Вважатимемо, що при наявності сенсора в зоні стабільного радіо покриття БПЛА, тобто при $(x_i, y_i) \in R$, миттєво відбувається зчитування даних моніторингу за певним протоколом взаємодії (наприклад, IEEE 802.15.4). Позначимо сумарний шлях, пройдений БПЛА по маршруту, через S.

Тоді можна сформулювати наступну постановку задачі: знайти такий маршрут польоту БПЛА (сукупність точок $\{x_j, y_j\}, j = \overline{1,K}$), який дозволяє в довільній послідовності покрити всі сенсори зоною радіо покриття радіусу R і при цьому мінімізувати сумарний шлях S. Математично це можна записати так:

$$M^0 = \underset{\substack{\{x_j,y_j\}\in R \\ \{x_i,y_i\}\in r \\ R<<r}}{\arg\min} S. \qquad (1)$$

При збігу точок маршруту БПЛА з точками розміщення сенсорів, тобто при $i=j$, дана задача представлятиме класичну геометричну задачу про комівояжера та може бути вирішена одним з відомих методів комбінаторної оптимізації (методи пожадливих алгоритмів, метод гілок і границь, метод повного перебору та ін.). Однак із зростанням кількості сенсорів поліноміально зростає складність та відповідно час вирішення задачі. Для вирішення цієї проблеми в роботі [15] запропоновано метод рекурсивного повного перебору, що дозволяє вирішувати задачу до 1000 вузлів за прийнятний час. Також для вирішення поставленої задачі можуть бути застосовані стандартні методи переміщення пошуково-рятувальних засобів (кораблів, літаків, вертольотів) при виконанні пошукових операції на морі або на суші – паралельні галси або квадрат, що розширюється (рис.1).

Однак рішення, отримані цими методами, будуть не завжди оптимальними. Наприклад, метод слідування по всім точкам розташування сенсорів буде неефективним при великій кількості вузлів, а пошукові методи будуть явно поступатися при малій кількості сенсорів. Отже виникає необхідність їх вдосконалення. Це можливе шляхом застосування певних евристичних підходів. Наприклад, буде доцільно слідувати не по всім точкам розташування сенсорів, а групувати сенсори по радіусу зони покриття БПЛА

і слідувати по центрам тяжіння цих груп. Таким чином ми будемо вирішувати ту ж саму задачу комівояжера, але меншої розмірності, заощаджуючи при цьому час розв'язання та пройдений БПЛА шлях.

Таким чином, удосконалений метод пошуку маршруту польоту БПЛА матиме наступний порядок:

1. Розбиття сенсорів на групи по радіусу зони покриття БПЛА, застосовуючи пожадливий підхід – послідовний відбір груп з максимальною кількістю сенсорів, що покриваються зоною радіо покриття БПЛА радіусу *R*.

2. Визначення центрів тяжіння груп сенсорів:

$$x_{0j} = \sum_{i=1}^{N^{\max}} \alpha_i x_i \,,\; y_{0j} = \sum_{i=1}^{N^{\max}} \alpha_i y_i \,,\quad (x_i, y_i) \in R \qquad (2)$$

де $\alpha_i = 1/N^{\max}$, $N^{\max}$ – кількість сенсорів максимальної групи. Також зазначимо, що $\sum_{i=1}^{N^{\max}} \alpha_i = 1$.

3. Вирішення задачі комівояжера на множині точок $\{x_{0j}, y_{0j}\}$, наприклад, методом рекурсивного повного перебору із застосуванням програмного забезпечення CommisVoyageur, розробленого автором роботи [15].

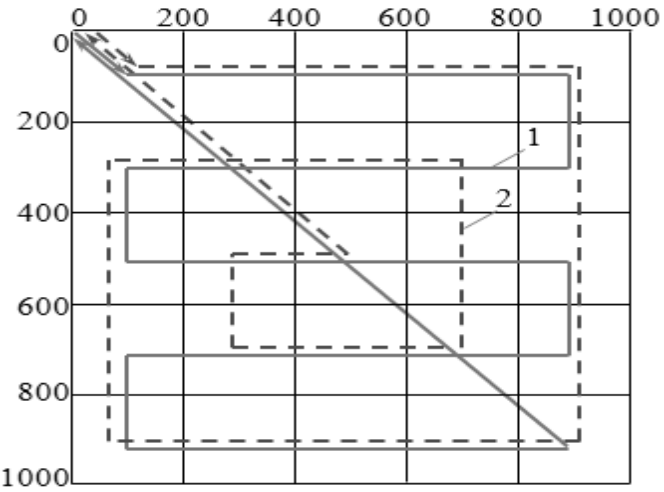


Рис. 1. Схеми пошуку: 1 – паралельні галси, 2 – квадрат, що розширюється.

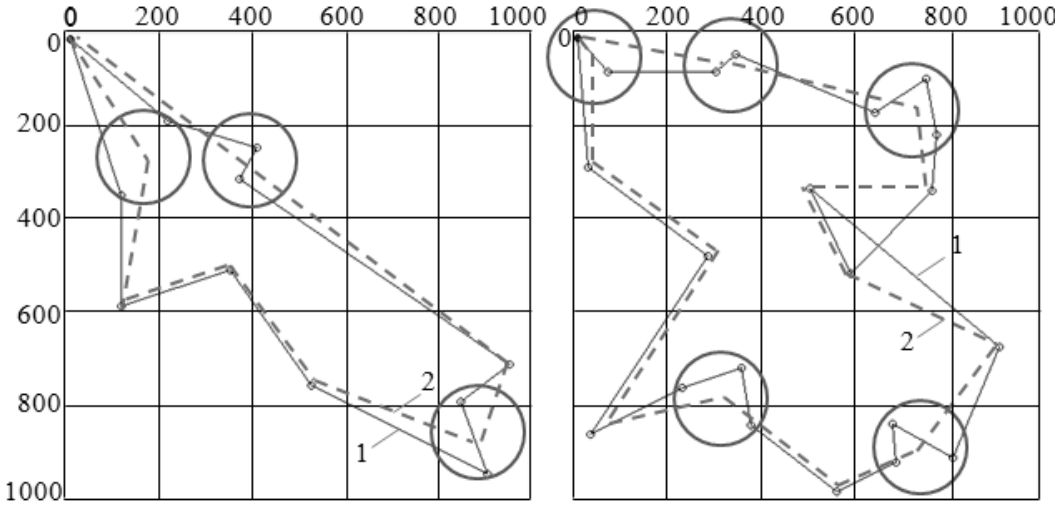
Проведено оцінку ефективності удосконаленого методу у порівнянні з методом слідування по всім сенсорам і методами пошуку (паралельні галси та квадрат, що розширюється).

Нехай задано вихідні дані: зона спостереження розміром r = 1000x1000 м; радіус зони стабільного радіо покриття R = 200 м; координати точок розміщення сенсорів $\{x_i, y_i\}, i = \overline{1, N}$, де N = 1…100, задають випадковим чином.

Використовуючи зазначені дані було побудовано маршрути польоту БПЛА методом слідування по всім сенсорам та удосконаленим методом слідування по центрам тяжіння груп сенсорів, як показано на рис.2. Маршрути польоту згідно методів пошуку будуть незмінними в залежності від кількості сенсорів і відповідатимуть схемам, вказаним на рис.1. Результати розрахунку сумарно пройденого шляху *S* від кількості сенсорів *N* згідно зазначених методів наведено на рис.3. Залежність кількість точок в маршруті *K* від кількості сенсорів *N* при різних методах збору інформації наведено рис.4.

Результати моделювання (рис.3) свідчать, що при малих значеннях *N* метод слідування по всім сенсорам і удосконалений метод слідування по центрам тяжіння

мають майже однакові результати через малу кількість груп. Однак із зростанням кількості сенсорів значну перевагу (до 17-23%) має удосконалений метод за рахунок збільшення кількості груп і відповідно зменшення кількості точок в маршруті (рис.4). При великій кількості вузлів (більше 60-70) доцільніше застосовувати один з методів пошуку.



а) б)

Рис. 2. Маршрути польоту БПЛА згідно методу слідування по всім сенсорам (1) і методу слідування по центрам тяжіння груп сенсорів (2) при N=10 (а) та N=20 (б).

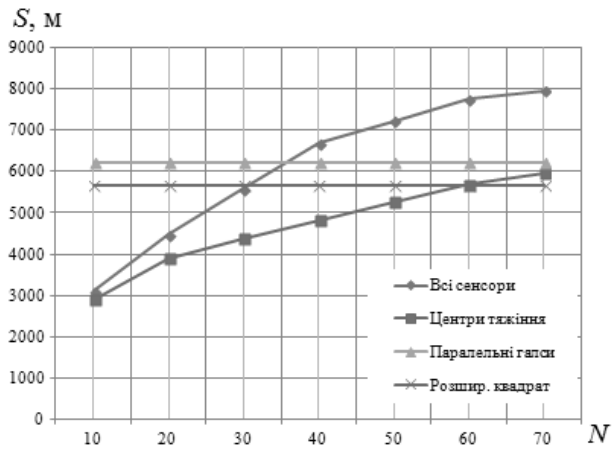


Рис.3. Графік залежності сумарного пройденого шляху S в залежності від кількості сенсорів N при різних методах збору інформації.

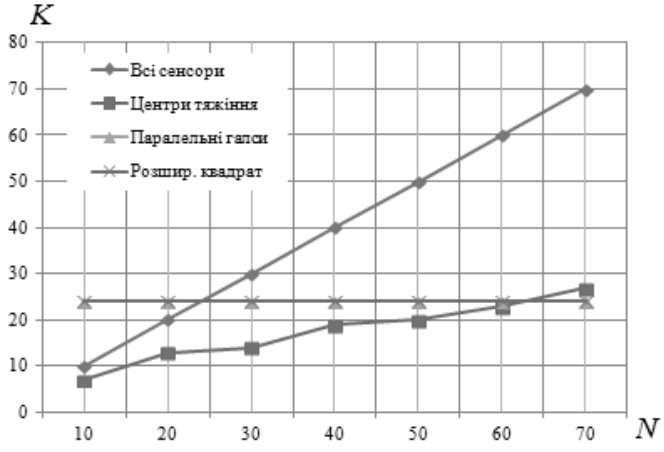


Рис.4. Графік залежності кількості точок в маршруті K в залежності від кількості сенсорів N при різних методах збору інформації.

Література

1. Drones PoC in telecom - du & Nokia joint initiative. http://www.mobileworldlive.com/featured-content/home-banner/nokia-networks-du-deploy-drones-test-network-performance/
2. Nokia “Drones for good” proposal. https://www.dronesforgood.ae/
3. Lysenko O.I., Valuiskyi S.V. Capacity increasing of sensor telecommunication networks / O.I. Lysenko, S.V. Valuiskyi // Telecommunication Sciences. – 2012. – vol. 3. – № 1. – P. 5–11.

Секція 1. Передавання інформації в телекомунікаційних системах

УДК 681.31

МЕТОДИ ТА АЛГОРИТМИ КОДУВАННЯ І ПЕРЕДАЧІ МОНІТОРИНГОВИХ ДАНИХ В ІНФОРМАЦІЙНО-ЕФЕКТИВНИХ РАДІОМЕРЕЖАХ

Шевчук Б.М.
Інститут кібернетики імені В.М. Глушкова НАН України, Україна
E-mail: incors@ukr.net

The methods and algorithms for coding and transmission of monitoring data in information-effective radio networks

The algorithms for improving of the packet data transfer efficiency in radio networks based on implementation by means of subscriber systems the adaptive and high-speed algorithms for the signals and images compact coding, for forming and transmission of code-signal sequence packets including noise-like are proposed.

Підвищення ефективності функціонування моніторингових радіомереж з пакетною передачею інформації суттєво залежить від методів і алгоритмів кодування первинних даних, що підлягають передачі, алгоритмів формування кодово-сигнальних послідовностей (КСП) інформаційних пакетів (ІП) з урахуванням рівня шумів в радіоканалі [1-3] та передачі ІП віддаленим абонентам радіомережі з використанням основного і резервних шляхів ретрансляції пакетів. Підвищення ефективності передачі ІП абонентськими системами (АС) досягається за рахунок мінімізації кількості передач ІП кожною АС, зменшенням їх тривалості при високій інформаційній ємності ІП. Передача ІП вирішується комплексно, на радіотехнічному та інформаційному рівнях обробки і передачі даних, включаючи за рахунок підвищення ефективності радіотехнічних засобів та шляхом реалізації процесорними засобами АС комплексу взаємодоповнюючих методів та алгоритмів оброблення та кодування сигналів і зображень [4,5], компактного та криптостійкого кодування двійкових масивів даних, формування компактних завадостійких КСП пакетів для реалізації прихованої та захищеної (криптостійкої та завадостійкої) передачі інформації в шумах радіоканалу [1,3]. Від якості цих алгоритмів в значній мірі залежать системні характеристики радіомереж, включаючи максимальна швидкість передачі інформації, оперативність, надійність і захищеність передачі ІП віддаленим абонентам мережі. Оскільки АС моніторингових радіомереж орієнтовані на тривале функціонування в режимі неперервного відбору, накопичення і передачі моніторингових даних при живленні від автономних джерел енергії то важливим завданням АС є мінімізація вхідних моніторингових потоків даних та їх перетворення у вихідні захищені дані, що підлягають накопиченню в об’єктних АС або

бортових засобах, наприклад, мобільних роботів чи безпілотних апаратів, а також передачі пакетів захищених даних в темпі введення даних або по запиту центральної станції або віддалених АС радіомережі. Ефективність передачі пакетів досягається зменшенням інформаційних потоків в місцях встановлення АС шляхом адаптації кодування вхідних даних в залежності від якості введення даних (відліки чистих від шумів ділянок сигналів кодуються з підвищеною частотою опиту і більш точно (максимальною більшість біт АЦП), а відліки ділянок з шумами кодуються мінімальною частотою опиту та мінімальною кількістю біт), формуванням пакетів, параметри КСП яких вибираються в залежності від рівня шумів в радіоканалі [1,3]. При заданій величині робочої смуги частот F максимальна канальна швидкість передачі інформації $R_{c\max} \le 2F/k_s$, де $k_s > 1.4...1.8$ – коефіцієнт, що враховує якість відновлення фронтів цифрових (імпульсних) сигналів. При заданій ймовірності помилкового прийому КСП P_n поточна швидкість передачі R_i є змінною і залежить від вибору ключових параметрів процесів введення, кодування та передавання даних, тобто $R_i = f(F, P_n, K_c(\delta_d^N), (E_{is}/J_0)_n, L/B(\gamma_i))$, де $K_c(\delta_d^N)$- коефіцієнт стиску даних на інформаційному рівні засобів АС, який залежить від допустимої величини рівня вхідних шумів δ_d^N в околиці суттєвих відліків (СВ) сигналів, стиску даних без втрат та від коефіцієнта зменшення тривалості пакетів [1,3], $(E_{is}/J_0)_n$- необхідне енергетичне співвідношення сигнал/шум в каналі зв'язку, $E_{is} = S \cdot T_{is}$, S- потужність сигналу, T_{is}- тривалість інформаційного сигналу (КСП), $J_0 = J/F$, J- середня потужність сумарних завад в радіоканалі ($(E_{is}/J_0)_n \approx (S/J)\cdot B$), $B = F \cdot T_{is}$- база канального сигналу (коефіцієнт розширення спектру сигналу), γ_i- поточне енергетичне співвідношення $(E_{is}/J_0)_i$, $L \le B/4$ – кількість ортогональних сигналів, які асиметрично можна передавати в загальному радіоканалі зі смугою F. Основою методів і алгоритмів якісного стиску та відновлення сигналів (відеосигналів) з допустимими втратами інформації є збереження характеристик обвідних сигналів з урахуванням вимог та особливостей прикладних завдань [4]. В процесі оперативної обробки і кодування сигналів на основі аналізу знаків різницевих значень ΔX_i^F і $\Delta(\Delta X_i^F)$ визначаються амплітудно-часові параметри найбільш інформативних відліків обвідних сигналів, де $\Delta X_i^F = X_i^F - X_{i-1}^F$ - поточний приріст сусідніх відліків X_i^F і X_{i-1}^F відфільтрованого сигналу, $i = \overline{1,v}$, нумерація вхідних відліків поточної вибірки сигналу, v- максимальна кількість відліків, які накопичуються в оперативній пам'яті процесорного модуля АС. В залежності від оперативно визначених опосередкованих оцінок вхідного співвідношення сигнал/шум в околиці СВ (глобальних екстремумів, локальних екстремумів, точок перегину) $\Delta X_{CBi}^N = \left| X_{CBi}^N - X_i \right|$ та в залежності від умов $\Delta X_{CBi}^N \le \delta_d^N$ або $\Delta X_{CBi}^N > \delta_d^N$, формуються стислі масиви різницевих амплітудно-часових параметрів СВ сигналів [4,5]. В подальшому отримані масиви підлягають оперативному

стиску без втрат [5] та криптозахисту з використання псевдовипадкових послідовностей, кодові ключі генерації яких відомі тільки абоненту-передавачу та абоненту-приймачу ІП. Після шифрування даних отримуємо криптомасив $Y = y_1,..., y_i,..., y_n$ (n – максимальна кількість біт масиву), для якого справедливий вираз $Y = X \oplus K$, де $X = x_1,..., x_i,..., x_n$ – послідовності бітів компактного масиву даних, $K = k_1,..., k_i,..., k_n$ – послідовності випадкових бітів, значення яких залежать від поточного секретного ключа, $y_1 = x_1 \oplus k_1,..., y_i \oplus k_i,..., y_n \oplus k_n$. Беззбиткові та криптостійкі масиви даних підлягають завадостійкому кодуванню та перемішуванню [4]. Ефективні методи та алгоритми передачі ІП в радіомережах реалізуються не основі перекодування n-бітових послідовностей, $n = \overline{3,8}$, в інтервальні КСП ІП, які, з урахуванням рівня шумів в радіоканалі [3,4], передаються дворівневими сигналами або шумоподібними сигналами (ШПС) з адаптивною базою B_a. При цьому швидкість передачі інформації збільшується приблизно в 2 рази при незмінній робочій смузі частот F. Для надійного прийому спотворених шумами КСП-ШПС кореляційним приймачем відповідного ШПС по трьом каналам здійснюється обчислення сумарної модульної функції $G_s(j) = G_b(j) + G_{a1}(j) + G_{a2}(j)$ з сумуванням відліків основного каналу $G_b(j)$ та додаткових каналів $G_{a1}(j)$ і $G_{a2}(j)$, де j-величина часового зсуву, при цьому обчислення по додаткових каналах здійснюється з використанням різних матриць розгортання і сумування модульних різниць вхідних і опорних ШПС.

З використанням розповсюджених радіомодулів, наприклад, ISM діапазону частот, шляхом реалізації на інформаційному рівні засобів АС радіомереж запропонованого комплексу алгоритмів оперативного кодування даних та формування високоінформативних КСП ІП досягається високошвидкісна та захищена передача пакетів інформації в шумах радіоканалу

Література

1. Shevchuk B.M. Speed-and Coding Accuracy-Optimal Methods and Algorithms to Increase the Operation of Wireless Network Subscriber Systems// Cybernetics and Systems Analysis, Vol. 50, No 6, 2014, pp.945-955.
2. Shevchuk B.M. Theoretical and Algorithmic Foundations of Improving the Efficiency of Packet Data Transmission in High-Speed and Secure Radio Networks// Cybernetics and Systems Analysis, Vol. 52, No 1, 2016, pp. 151-159.
3. Шевчук Б.М., Задірака В.К., Фраєр С.В. Підвищення ефективності передачі інформації в моніторингових мережах на основі оптимізації обчислень в процесі кодування даних засобами об'єктних систем сенсорних мереж// УСіМ. – 2015. - №3. – С. 65-71.
4. Шевчук Б.М. Системний підхід до вирішення проблем оптимізації обчислень засобами об'єктних систем сенсорних мереж// Інформаційні технології та комп'ютерна інженерія. – 2013. - № 1. – С. 88-95.
5. Шевчук Б.М., Задірака В.К., Фраєр С.В. Алгоритмічні основи підвищення інформаційної ефективності передачі даних в сенсорних мережах// Комп'ютерні засоби, мережі та системи. – 2013. – №12. – С. 140-149.

УДК 621.391.8

АНАЛІЗ ПРИНЦИПІВ ФОРМУВАННЯ ТА КОРИГУЮЧИХ МОЖЛИВОСТЕЙ КАСКАДНИХ КОДІВ

Пєшкін А.М., Уривський Л.О.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: antonmp90@mail.ru

Analysis of construction principles and error correcting capabilities of concatenated codes

Construction principles and main parameters of concatenated codes are presented. The new algorithm of error correcting ability of concatenated codes is proposed. Based on proposed algorithm well known 802.16 concatenated code correcting abilities are evaluated.

В 1966 році для отримання завадостійких кодів із значною довжиною блоку коду n та високою коригуючою здатністю Форні були запропоновані каскадні коди. Велика еквівалентна довжина блоку досягається завдяки введенню декількох ступенів кодування.

Метою даної роботи є оцінка реальної завадостійкості каскадних кодів за допомогою знаходження еквівалентного каскадному блокового коду.

Розглянемо найбільш розповсюджену схему каскадного коду, що складається з двох ступенів. В якості зовнішнього коду, як правило, використовується недвійковий код Ріда-Соломона, а в якості внутрішнього – згортковий код, або двійковий блоковий код.

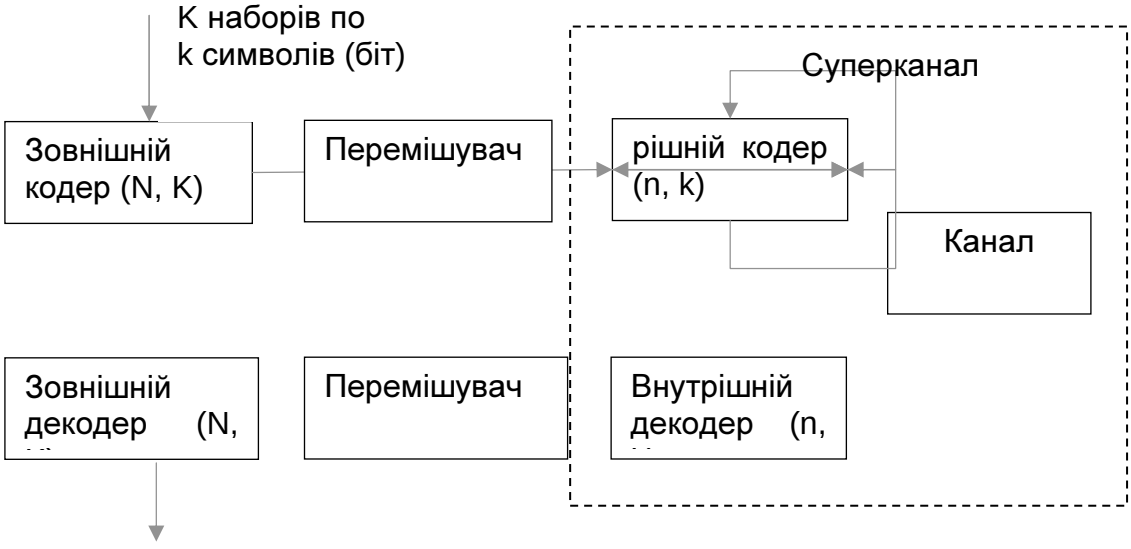


Рис.1 Схема кодування каскадним кодом із двома ступенями кодування.

Між зовнішнім та внутрішнім кодерами знаходиться перемішувач, який необхідний для боротьби з груповими помилками та може використовуватися для узгодження розмірності недвійкових символів внутрішнього і зовнішнього кодів.

У найпростішому випадку в якості зовнішнього та внутрішнього кодерів використовуються блокові коди. Нехай зовнішній код визначається параметрами (N, K, $d_{зовн}$), а внутрішній код, відповідно, (n, k, $d_{вн}$). Для

формування каскадного коду на перший кодер подається K наборів по k біт (рис. 2).

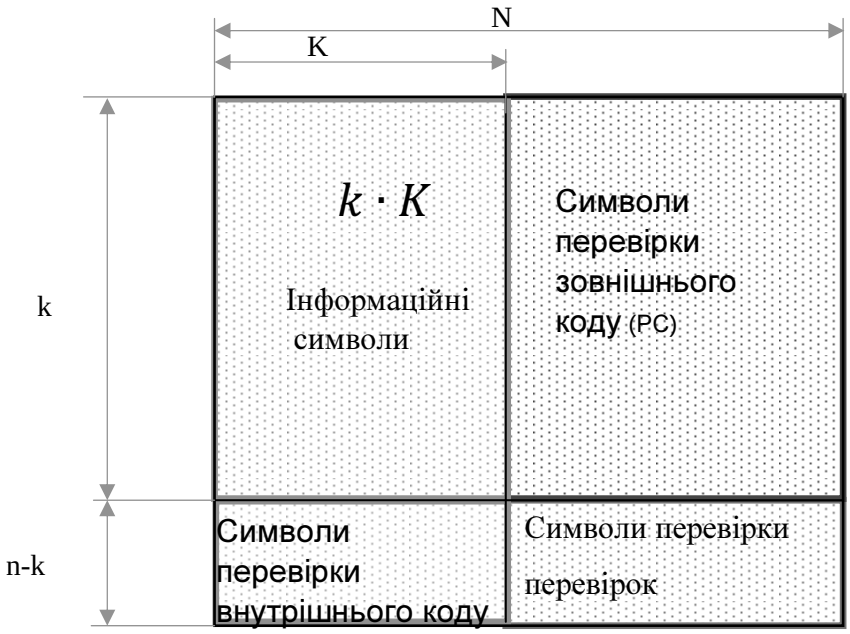


Рис.2 Зображення принципу формування кодового слова каскадного кода.

Кожен з наборів являє собою інформаційний символ, а розмір алфавіту зовнішнього коду, таким чином, складає $q=2^k$. Після кодування першим кодером на його виході формується код Ріда-Соломона довжиною N. Далі послідовність потрапляє у перемішувач, та далі на вхід другого кодера, куди подається N наборів по k біт (N символів), кожен з яких кодується внутрішнім кодом довжиною n. В результаті у канал звязку потрапляє кодована послідовність довжиною $N^* = n \cdot N$, з яких $K^* = k \cdot K$ – інформаційні біти [2]. Кодова швидкість буде дорівнюватись добутку кодових швидкостей внутрішнього та зовнішнього коду $R^* = \frac{k \cdot K}{n \cdot N}$. Отриманий у результаті каскадний код є лінійним, та його кодова відстань не менша від добутку кодових відстаней складових кодів [1]:

$$d^* \geq d_{\text{зовн}} \cdot d_{\text{вн}} \qquad (1)$$

Більш складною є оцінка завадостійкості каскадного коду, де в якості внутрішнього виступає згортковий код. Розглянемо алгоритм визначення завадостійких характеристик каскадного коду на прикладі реального коду, який використовуються у технології IEEE 802.16x. В якості зовнішнього використовується код Ріда-Соломона (32, 24, 9), сформований на основі поля GF(8). Тоді в бітовому представлені параметри коду будуть відповідно (256, 192, 9). В якості внутрішнього згідно стандарту використовується код зі швидкістю $\mathrm{R} = \frac{2}{3}$ та довжиною кодового обмеження $D = 8$. Результуюча швидкість дорівнює $R = \frac{2}{3} \cdot \frac{24}{32} = \frac{1}{2}$.

Для оцінки завадостійкості даної конструкції можливо використовувати наступний алгоритм, метою якого є визначення блокового коду, еквівалентного каскадному:

1. Знаючи вимоги до достовірності передачі $P = 10^{-6}$, визначити ймовірність помилки P_S в каналі зі згортковим кодом.

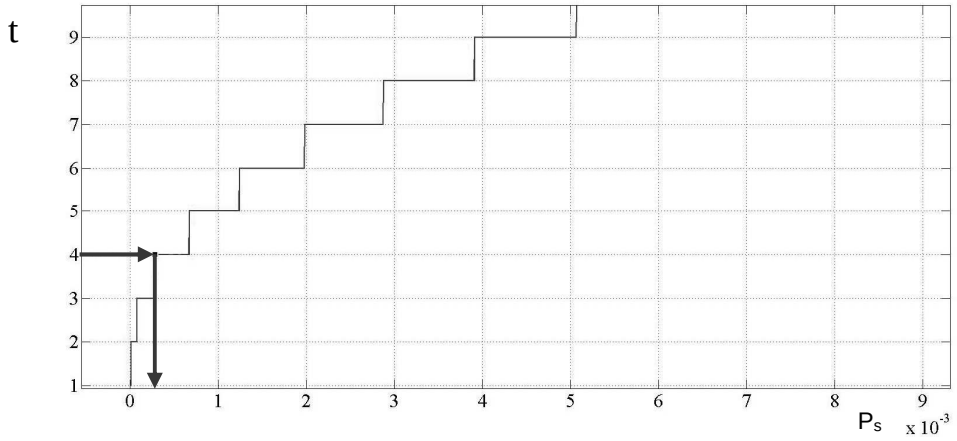


Рис.3 Зображення залежності кількості виправляємих помилок t від ймовірності помилки у каналі p для фіксованої ймовірності помилки на виході декодера $\boldsymbol{P = 10^{-6}}$.

Для обраного зовнішнього коду з t=4 ймовірність помилки на виході відповідного каналу буде $P_S = 2.79 \cdot 10^{-4}$

2. Використовуючи в якості вимоги до достовірності P_S, визначити максимально допустиму ймовірність помилки p в каналі з неперервним кодом за допомогою ліній завадостійкості (рис. 4).

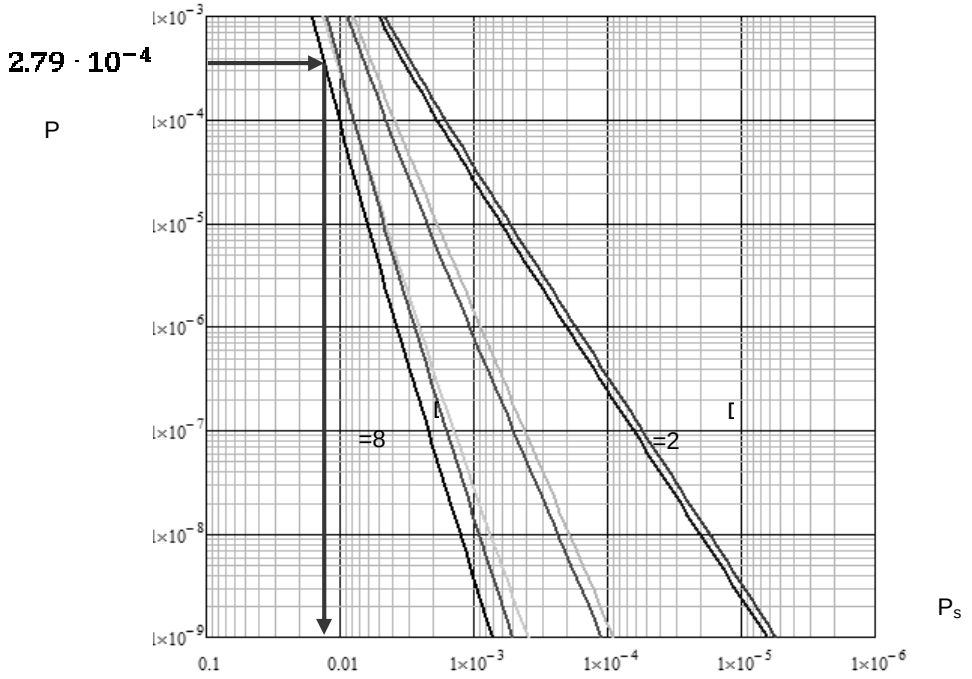


Рис.4 Зображення залежності ймовірності помилки на виході декодера неперервного коду від канальної ймовірності помилки для $R = \frac{2}{3}$ та при використанні жорсткого декодера Вітербі для різних D ϵ{2,3..8} [3].

Згідно рис.4 при використанні обраного згорткового коду найгірша канальна ймовірність помилки може бути $p = 1.5 \cdot 10^{-2}$

3. При відомих параметрах канальної ймовірності помилки p та вимог до достовірності $P = 10^{-6}$ знайти довжину блоку еквівалентного блокового коду, який забезпечив би задану достовірність та мав би еквівалентну кодову швидкість. Параметри еквівалентного коду і будуть параметрами каскадного коду.

Згідно отриманих результатів еквівалентний блоковий код має забезпечувати достовірність $\mathrm{P} = 10^{-6}$ при канальній ймовірності помилки $\mathrm{p} = 1.5 \cdot 10^{-2}$ та мати кодову швидкість $\mathrm{R} = \frac{2}{3} \cdot \frac{24}{32} = \frac{1}{2}$. Використовуючи методику пошуку оптимального завадостійкого коду за критерієм максимального наближення до границі Шеннона [4] можна визначити, що довжина еквівалентного блокового коду за границею Варшамова-Гільберта може бути n=256. З огляду на те, що знайдений еквівалентний блоковий код є найефективніший з гарантованою реалізацією (знаходиться на границі Варшамова-Гільберта), а каскадний код має значно гірші показники коригувальної ефективності, слід зробити висновок, що перевагою каскадних кодів перед блоковими є спрощена процедура формування та декодування.

Висновки. В даній роботі виконана оцінка основних параметрів каскадних кодів. Приведений алгоритм визначення найгіршого каналу, для якого каскадний код може забезпечити необхідну достовірність. Також розроблений алгоритм визначення параметрів еквівалентного блокового коду за критерієм рівності кодової швидкості та виправної здатності та з використанням границі Варшамова-Гільберта. Згідно отриманих результатів еквівалентним кодом каскадному коду із зовнішнім кодом (32, 24, 9) та внутрішнім неперервним кодом $R = \frac{2}{3}$ та $D = 8$ може бути блоковий код зі швидкістю $R = \frac{2}{3} \cdot \frac{24}{32} = \frac{1}{2}$ та довжиною блоку n=256, що дорівнює довжині блоку зовнішнього коду Ріда-Соломона. Таким чином, можна зробити висновок, що гарантовано існують блокові коди з n>256, які дозволяють отримати кращу достовірність, або інформаційну ефективність. Використання каскадних кодів є більш простим підходом з точки зору реалізації кодерів та швидкості кодування.

Розвиток технологій швидкісної обробки кодів спонукає використовувати блокові коди з великою довжиною блоку замість каскадних кодів для підвищення ефективності використання ресурсів каналу зв’язку.

Література

1. Р. Морелос-Сарагоса. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / Москва: Техносфера, 2005. – 320с
2. Кларк Дж., Кейн Дж. Кодирование с исправлением ошибок в системах цифровой связи/ Пер. с англ. – М.: Радио и связь, 1987. – 392 с.
3. Оцінка граничних корегуючих можливостей неперервних кодів через еквівалентні параметри блокових кодів/ Л. О. Уривський, А. М. Пєшкін// Збірник тез сьомої міжнародної науково-практичної конференції «Проблеми телекомунікацій-2013»
4. Оптимальные помехоустойчивые коды по критерию максимального приближения к границе Шеннона. /Урывский Л. А., Пешкин А.М. /Сборник тезисов Шестой международной научно-практической конференции «Проблемы телекоммуникаций - 2012»

УДК 621.391

СИНТЕЗ МЕТОДИКИ ОЦЕНКИ КАЧЕСТВА ЦИФРОВОГО СИГНАЛА

Мошинская А.В., Георгин Д.А.
Институт телекоммуникационных систем НТУУ «КПИ», Украина
E-mail: avmoshinskaya@gmail.com, d-georgin@yandex.ua

Synthesis of method for quality estimation of digital signal

The new technique for quality estimation of digital signal is proposed. The parameters for quality of digital signal from ITU-T Rec. G.826 are investigated in this paper. Relationship between theoretical and applied knowledge is found.

Категория «качество передачи цифрового сигнала» является одной из важных характеристик при оценке эффективности передачи информации в телекоммуникационной системе. В классических трудах В.И. Коржика, Л.М. Финка и др. качество передачи сигнала обуславливается помехоустойчивостью канала связи и определяется достоверностью передачи информации [1,2]. Показателями достоверности выступают вероятность ошибки символа в канале связи $p_{ош}$ и вероятность ошибки информационного бита $p_б$ [4].

Целью исследования является создание такой единой методики оценки качества связи, в которой знания, предлагаемые в теории помехоустойчивости и выраженные аналитическими закономерностями, можно сделать прикладными с помощью современных рекомендаций союза электросвязи ITU-T.

Предлагаемая методика синтезируется на основе предлагаемой аналитики теории помехоустойчивости и результатах современных стандартов ITU, которые предлагают инструментальные измерения.

В рекомендации G.826 определены три типа блочных ошибок:

- ошибочный блок (Errored block, EB), содержит один или более ошибочных битов (информационных либо проверочных);
- секунда с ошибками (Errored Second, ES), содержащая хотя бы один блок с ошибками или дефект;
- секунда с многочисленными ошибками (Severely Errored Second, SES), содержащая 30% блоков с ошибками или, по крайней мере, один период с серьезными нарушениями соединения (Severely Disturbed Period, SDP); [3]

Аналитические зависимости для определения параметров качества связи строятся на основе известной вероятности искажения одного бита (информационного либо проверочного), то есть вероятности ошибки непрерывного потока бит ***p***.

Вероятность возникновения ошибочного блока равна вероятности события, что хотя бы один из ***n*** *бит в блоке искажен:*

$$P(EB) = 1 - (1 - p)^n \quad (1)$$

Предполагается, что в одну секунду передается количество блоков ***M***, являющееся целым числом. Таким образом, за одну секунду передается ***M*** блоков по ***n*** бит. С другой стороны количество бит за секунду – это скорость ***V***. Следовательно,

$$M = V / n \quad (2)$$

Зная количество блоков за секунду (2), а также вероятность того, что блок ошибочен (1), можно записать формулу:

$$P(ES) = 1 - (1 - P(EB))^M \quad (3)$$

- вероятность события, что хотя бы один блок в течение секунды был ошибочным.

Необходимо сделать уточнение, что блок, попавший в две соседние секунды сразу, будет влиять на обе секунды при идентификации их ошибочности. Следовательно, количество блоков в секунду, рассчитанное по формуле (2) всегда будем округлять до целого в большую сторону.

Зная количество блоков за секунду (2), а также вероятность того, что блок ошибочен (1), и используя *биномиальное распределение*, можно определить вероятность появления определенного количества ошибочных блоков за одну секунду.

Пусть ***y*** – количество ошибочных блоков секунде,

$$y = 0, 1, 2...M, \quad (4)$$

тогда

$$P(y = k) = \frac{M!}{(M-k)!k!} P(EB)^M (1 - P(EB))^{M-k} \quad (5)$$

Для возникновения секунды с многочисленными ошибками

необходимо, чтобы 30% и более блоков в секунде были ошибочными, т.е.

$$y \geq 0.3M\ , \tag{6}$$

Тогда, используя (2) и (5) с учетом условий (4) и (6), запишем

$$P(SES) = 1 - \sum_{k=0}^{k<0.3M} P(y = k), \tag{7}$$

где вычитаемое – это сумма вероятностей событий, каждое из которых заключается в появлении количества ошибочных блоков в данной секунде меньшего, чем 30%.

Таким образом, предлагается новая методика оценки показателей качества каналов телекоммуникаций. Задаваясь исходными данными, а именно скоростью источника $\boldsymbol{V}$, размером блока $\boldsymbol{n}$ и вероятностью ошибки символа $\boldsymbol{p}$ можно определить вероятность появления ошибок в одном блоке и вероятность появления одного или более ошибочных блоков в передаваемой последовательности символов, приводя теоретические показатели помехоустойчивости к стандартизированным показателям достоверности в телекоммуникационных системах.

Литература

1. Коржик В. И., Финк Л. М., Щелкунов К. Н. Расчет помехоустойчивости систем передачи дискретных сообщений: Справочник /: Под ред. Л. М. Финка. — М.: Радио и связь, 1981. — 232 с.
2. J. G. Proakis, Digital Communication, 4th ed. Boston, MA: McGraw-Hill, 2000.
3. ITU-T Recommendation G.826. End-to-end error performance parameters and objectives for international, constant bit-rate digital paths and connections, – 2002. – pp. 6-9.
4. Мошинская А.В. Методика оценки качества цифрового сигнала // А.В. Мошинская, Л.А. Урывский - «Проблеми телекомунікації»: дев’ята міжнародна науково-технічна конференція, присвячена дню науки в Україні (ПТ-15) 21-24 квітня 2015 р., К.: с. 68…71

УДК 621.382

ИССЛЕДОВАНИЕ КАЧЕСТВЕННЫХ ХАРАКТЕРИСТИК VOIP

Прокушев А.Н., Ступак Г.В., Бойко В.В.
Донецкий национальный технический университет, Украина
E-mail: AND9ua@yandex.com

RESEARH OF VOIP QUALITY

The article presents a model of Quality of Service research for VoIP, which can be used for further design of communication networks. This model can be useful both to network developers and service providers.

В современном мире все большую популярность приобретает услуга VoIP. Она позволяет рационально использовать пропускную способность сети и объединять в одном канале голос и данные. Использование IP-сетей для передачи голосового трафика требует гарантированных параметров качества обслуживания (QoS), а их обеспечение зависит в первую очередь от понимания того как оценивать качество и какие параметры сети оказывают наибольшее влияние [1]. Работа преследует две цели – проверить экспериментальным путем методику оценки полосы пропускания для одного разговорного тракта VoIP [2] и оценить степень влияния загруженности сети на качественные параметры разговорного тракта. Для проведения натурных исследований предложено использовать следующую схему (Рисунок 1).

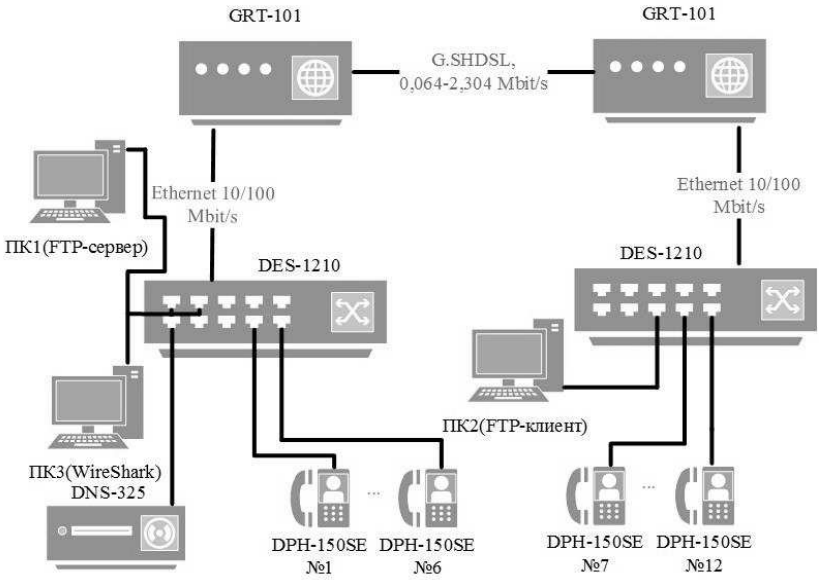


Рис.1 Схема исследования QoS для VoIP.

Данная схема включает в себя два сегмента сети, построенных на базе управляемых коммутаторов D-Link DES-1210, IP-телефонов – D-Link DPH 150SE, IP-АТС Asterisk на базе DNS-325. Сегменты объединены низкоскоростным каналом с пропускной способностью в диапазоне 64-2304 Кбит/с с шагом 64 Кбит/с (модемы Planet GRT-101). Загрузку сети

обеспечивают две рабочие станции (передача FTP трафика), а измерения – на базе персонального компьютера с WireShark. Предложенная схема исследования позволит оценить такие показатели QoS как: максимальная пропускная способность, задержка, джиттер, потеря пакета.

Проверим правильность методики расчета [2], согласно которой аналитическим путем можно оценить некоторые параметры QoS, в том числе и требуемую пропускную способность. Для проведения расчетов в соответствии с [2] в качестве кодека будет использован G.711 (полезная битовая скорость 64 Кбит/с) с длительностью семпла 20 мс. Полный цикл передачи одного пакета IP-телефонии включает в себя следующие элементы (при использовании канальной технологии Ethernet): межкадровый интервал — 96 бит, преамбула — 64 бит, заголовок II уровня с учетом контрольной суммы — 144 бит, заголовок III уровня — 160 бит, заголовок IV уровня — 64 бита, заголовок V уровня — 96 бит, полезная нагрузка.

Полезная нагрузка рассчитывается, исходя из заданной битовой скорости кодека и времени семпла:

$$b_{полезн} = r \cdot t_s$$
$$b_{полезн} = 64 \cdot 10^3 \cdot 20 \cdot 10^{-3} = 1280 бит \quad (1)$$

Поскольку период следования пакетов равен времени семпла, то пропускная способность, необходимая для 1 разговора, определяется:

$$B_{абон} = \frac{b_{полезн} + \sum b_i}{t_s}$$
$$b_{полезн} = \frac{1904}{20 \cdot 10^{-3}} = 95{,}2 Кбит/сек \quad (2)$$

Проверим экспериментальным путем полученное значение пропускной способности в 95,2 Кбит/с. Установим значение пропускной способности GRT-101 на максимальном уровне, проведем разговор длительнотью 60с, и при помощи WireShark захватим пакеты на сетевом интерфейсе Asterisk. Общее количество RTP-пакетов составило 3021, количество отброшенных 0. В результате обработки захваченных пакетов было получена усредненное значение пропускной способности 85 Кбит/с, что подтверждает правильность методики [2] и возможность ее использования для оценки требуемой полосы в VoIP-сетях. Незначительные отличия реальных и аналитических величин легко объясняется тем, что при экспериментальной оценке пропускной способности WireShark не учитывает преамбулу и контрольную сумму.

Перейдем к серии экспериментов, которые позволят достигнуть следующую цель работы, а именно оценить степень влияния загруженности канала на показатели качества установленного соединения. Эксперимент состоит из двух частей, первая заключаться в серии опытов, в ходе которых будет увеличиваться количество разговорных трактов вплоть до того момента, когда показатели достигнут критических значений, и вторая – во время разговора начать передачу FTP-трафика и оценить изменение параметров QoS. Пропускную способность GRT-101 установим 256 Кбит/с.

В качестве критерия оценки будет выступать 5-ти бальная шкала MOS (Mean Opinion Score), с количеством экспертов 5 человек. Основные результаты первой части эксперимента приведены в таблице 1.

Таблица 1 Результаты первой части эксперимента.

Кол-во разгов.	*Требуемая полоса пропускания, Кбит/с*	*MOS*	*Наблюдаемый эффект*
1	95,2	5	Речь воспринимается полностью и без искажений, без задержки.
2	190,4	4-4,5	Речь воспринимается полностью и без искажений, без задержки, незначительные шумы.
3	286,6	1,5-2	После окончания разговора 1 телефон потерял регистрацию. Речь воспринимается с усилиями, заметная задержка.
4	380,8	1	Последний 4-й разговор было невозможно осуществить. После окончания разговора 3 телефона потеряли регистрацию. Плохо слышна речь, до абонента доходят обрывки слов что указывает на потерю пакетов, большая задержка.

Оценки 3,5 баллов и выше соответствуют стандартному и высокому телефонному качеству, 3,0…3,5 - приемлемому, 2,5…3,0 - синтезированному звуку [3].

Во второй части опыта при разговоре двух абонентов, нагружаем сеть еще и FTP-трафиком, происходит полная загрузка канала, что приводит к возникновению задержки 3-5 секунд в разговоре. Передача FTP трафика будет осуществляться при очень низкой скорости или процесс будет прерван. При такой занятости канала инициация второго вызова становиться невозможна.

Исходя из доводов, приведенных в статье, и проведенных экспериментов, можно сделать вывод о том, что методика расчета [2] верна и это подтверждено экспериментальным путем. Был выявлен эффект взаимного и негативного влияния FTP трафика в канале связи на IP-телефонию. Это в первую очередь связано с отсутствием механизмов обеспечения QoS. Дальнейшая робота будет направлена на исследование поведения трафика VoIP при аналогичных условиях но с реализованными механизмами QoS.

Литература

1. *Гольдштейн Б.С.* «IP-телефония» (третье издание) / Гольдштейн Б.С., Пинчук А.В., Суховицкий А.Л. - М.: Радио и связь, 2006. — 336 с.: ил.
2. *Мукімов Ш.С.* Розрахунок пропускної здатності каналів зв'язку для корпоративних мереж / Ш.С. Мукімов, В.В. Бойко // Наукові праці Донецького національного технічного університету. - 2015. - № 1. — С. 113-122
3. *Назаров А.Н.* Модели и методы исследования процессов функционирования и оптимизации построения сетей связи следующего поколения / Назаров А.Н., Сычев К.И.- «Электросвязь», 2011. - № 3. — С. 43–49.

УДК 621.382

ХАРАКТЕРИСТИКИ ОЦІНКИ ЯКОСТІ СТЕГОСИСТЕМ

Шостак Н.В.
Харківський національний університет радіоелектроніки, Україна
E-mail: Natasha9246@yandex.ru

Characteristics of quality assessment stehosystem

Reviewed steganosystem as a transmission system. Methods of hiding information in fixed images are studied. Characteristics of the steganosystem using different methods of embedding are presented.

Способи і методи приховування секретних повідомлень відомі з давніх часів, причому, дана сфера людської діяльності отримала назву стеганографія. Стеганографія - один із способів захисту інформації від несанкціонованого доступу, у системах моніторингу мережевих ресурсів, а також для захисту авторських прав на деякі види інтелектуальної власності та для автентифікації цифрових об'єктів [1]. В якості носія прихованої інформації в роботі використовується зображення, що допускає спотворення власної інформації, які не порушують його функціональність.

Один із методів приховування інформації в просторовій області є метод Куттера-Джордана-Боссена [2]. Цей метод полягає у вбудовуванні повідомлення в канал синього кольору зображення, що має кодування RGB. Функції вбудовування і видобування в даному алгоритмі не симетричні, тому правильне розпізнавання біта повідомлення хоч і є високоймовірним, але не стовідсоткове.

Для вбудовування інформації в контейнер використовуватися синій колір заданого контейнера-зображення. Зображення будемо розглядати в колірній моделі RGB.

Розглянемо алгоритм передачі одного біту прихованої інформації в цьому методі. Нехай M_i – біт, що підлягає вбудовуванню, $C=\{R,G,B\}$ – зображення-контейнер, $p=(x,y)$ - псевдовипадковий піксель контейнера, у який буде виконуватись вбудовування.

Таємний біт M_i вбудовується в канал синього кольору шляхом модифікації яскравості - $\lambda_{x,y} = 0{,}29890 \cdot R_{x,y} + 0{,}58662 \cdot G_{x,y} + 0{,}11448 \cdot B_{x,y}$

Інший метод приховування інформації в просторовій області – метод Дармстедтера-Делейгла-Квісквотера-Макка. Цей метод є блочним методом вбудовування в просторову область контейнера. Перед вбудовуванням інформація перетворюється в вектор двійкових даних. Кожний біт вбудовується в окремий блок пікселів розмірність якого складає 8×8 (для забезпечення відповідності блокам, що використовуються під час JPEG-компресії). Таким чином, дія компресії рівномірно розподіляється на кожен вбудований біт, а зважаючи на збитковість вбудовування зростає загальна стійкість стегосистеми. Розглянемо процес вбудовування біт повідомлення більш детально. Процес вбудовування виконується в чотири етапи:

1. Розбиття масиву зображення-контейнера на блоки 8×8 пікселів.

2. Класифікація пікселів окремого блока на зони з приблизно однорідним значенням яскравості.

3. Розбиття кожної зони на категорії відповідно до індивідуальної (псевдовипадкової) маски.

4. Вбудовування біта в залежності від співвідношення між середніми значеннями категорій кожної зони шляхом модифікації значень яскравості кожної категорії в кожній зоні.

Вилучення вбудованої інформації з контейнера вимагає наявності відомостей про розмірності блоків, на які розбивається зображення, а також про конфігурацію масок, які використовувалися при вбудовуванні. Процес вилучення складається з наступних етапів:

1. Розбиття зображення на блоки розмірністю NxN.
2. Класифікація пікселів окремого блоку на зони.
3. Розподіл кожної зони на категорії.
4. Зіставлення середніх значень яскравості для визначення значення вбудованого біта даних.

Один з найбільш поширених на сьогодні методів приховування конфіденційної інформації в частотній області зображення полягає у відносній заміні величин коефіцієнтів ДКП [3]. Спочатку зображення розбивається на блоки розмірністю 8×8 пікселів. ДКП застосовується до кожного блоку, в результаті чого утворюються матриці 8×8 коефіцієнтів ДКП. Кожний блок з яких призначений для приховання одного біту даних. Недоліком цього методу є висока складність обчислення ДКП. Розглянемо метод більш детально.

На початковому етапі первинне зображення розбивається на блоки розмірністю 8×8 пікселів. ДКП застосовується до кожного блоку, в результаті чого отримують матриці 8×8 коефіцієнтів ДКП, де b - номер блоку контейнера C, a - позиція коефіцієнта в цьому блоці. Кожен блок при цьому призначений для приховання одного біта даних.

Під час організації прихованого каналу абоненти повинні попередньо домовитися про два конкретні коефіцієнти ДКП з кожного блоку, які будуть використовуватися для приховування даних. Зазначені коефіцієнти повинні відповідати косинус-функції з середніми частотами, що забезпечить прихованість інформації в суттєвих для ЗСЧ областях сигналу, до того ж інформація не буде спотворюватися при JPEG-компресії з малим коефіцієнтом стиснення.

Бенгам (D. Benham), Мемон (N. Memon), Ео (B.-L. Yeo) і Юнг (M. Yeung) запропонували оптимізовану версію методу відносної заміни величин коефіцієнтів ДКП(методу Коха-Жао). Причому оптимізація була проведена ними за двома напрямками: по-перше, було запропоновано для вбудовування використовувати не всі блоки, а лише найбільш підходящі для цього, по-друге, в частотній області блоку для вбудовування вибираються не два, а три коефіцієнти ДКП, що, як буде показано надалі, істотно зменшує спотворення контейнера.

Стеганографія може бути застосована для приховання зв’язку, захисту

авторських прав на зображення (автентифікація), відбитків пальців (відстеження порушника) додавання заголовків до зображень, додавання додаткової інформації, такої як субтитри до відео, захисту цілісності зображень (виявлення випадків шахрайства), управління копіюванням при DVD записі та в інтелектуальних браузерах, для автоматичного надання інформації про авторські права. Всі ці наведені методи проаналізовані і оцінені з використанням такого набору характеристик, які є показниками якості:

- пропускна здатність – кількість бітів прихованого повідомлення, які можуть бути передані за допомогою цього методу в зображенні фіксованого розміру. При цьому приховуване повідомлення повинне бути безпомилково передане одержувачу і захищене від атак порушника, таких як спроби виявлення факту наявності каналу прихованої зв'язку, читання прихованого повідомлення, навмисного введення помилкового повідомлення або руйнування вбудованої в контейнер інформації [4].

- стійкість – здатність вилучити приховану інформацію після загальних операцій з обробки зображень: лінійні і нелінійні фільтри, стиснення з втратами, регулювання контрастності, перефарбування, передискретизації, масштабування, обертання, додавання шуму, обрізки, друку/копіювання/сканування, перестановки пікселів у малій околиці, квантування кольорів тощо;

- невидимість – перцепційна прозорість, що спирається на властивості зорової або слухової системи людини;

- захищеність – характерна властивість, яка означає, що вбудована інформація не може бути видалена цілеспрямованими атаками, заснованими на відомому алгоритмі вбудовування та вилучення і знанні принаймні одного носія з прихованим повідомленням;

- складність вбудовування і виявлення – кількість стандартних операцій, які будуть виконані для вбудовування і виявлення прихованого повідомлення.

Напрямком подальших досліджень є вибір переважного методу приховування інформації в стегосистемі з використанням багатокритеріального підходу.

Література

1. В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. Цифровая стеганография. – М.: «Солон-Пресс», 2002. – 272 с.
2. M. Kutter, F. Jordan, F. Bossen, Digital Signature Of Color Images Using Amplitude Modulation //Proc.Of the SPIE Storage and Retrieval for Image and Video Databases V. 1997. Vol. 3022. Pp. 518-526.
3. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. – К.: МК-Пресс, 2006. – 288 с.
4. Cox, I., Miller, M., Bloom, J., Fridrich, J., Kalker, T. Digital Watermarking and Steganography. Second Edition. (Elsevier, 2008).

УДК 004.725

ДОСЛІДЖЕННЯ ДОЦІЛЬНОСТІ ВИКОРИСТАННЯ МЕТОДІВ ТЕОРІЇ ПРИЙНЯТТЯ РІШЕНЬ ПРИ СИНТЕЗІ МЕРЕЖ ДОСТУПУ

Гайворонська Г.С., Брицький С.В.
Одеська національна академія харчових технологій, Україна
E-mail: warriormagistr@gmail.com

Research the feasibility of using the methods of the theory of decision-making during the synthesis of access networks

The work is aimed at improving the efficiency of the synthesis of access networks. It is proposed by applying methods of the theory of decision making while solving individual tasks, which arise in the synthesis process of access networks.

Робота направлена на підвищення ефективності синтезу мереж доступу. Це пропонується здійснити шляхом застосування методів теорії прийняття рішень при вирішенні окремих задач, які виникають в процесі синтезу мереж доступу.

Для цього розроблено модель дослідження доцільності використання методів теорії прийняття рішень при синтезі мереж доступу, представлену на рис. 1. Методи теорії прийняття рішень проаналізовано з точки зору їх застосовності при синтезі мереж доступу, при врахуванні параметрів мережі доступу, які є вхідними при її синтезі. В результаті визначено методи теорії прийняття рішень, які доцільно застосовувати в процесі синтезу мереж доступу та розроблено рекомендації, щодо їх застосування.

В процесі виконання роботи визначено, що методи теорії прийняття рішень доцільно застосовувати до трьох задач синтезу, які пов’язано з визначенням:

- топологічної структури мережі доступу;
- технологій передачі даних по лініям доступу;
- обладнання, яке реалізуватиме вузли доступу.

При вирішенні кожної з сформульованих задач для них сформульовано мету, яку повинні задовольняти вибрані методи, проаналізовано самі методи на відповідність цій меті та визначено шість методів теорії прийняття рішень, які задовольняють поставлені до них вимоги.

Для задачі визначення топологічної структури мережі доступу вибрано три методи: аналізу ієрархій, дерева рішень та динамічного програмування.

Для задачі визначення технологій передачі даних по лініям доступу – два методи: послідовного вводу обмежень та ідеальної точки.

Для задачі визначення обладнання, яке реалізуватиме вузли доступу – метод вибору за кількістю домінуючих критеріїв.

Після цього визначено технології передачі даних по лініям доступу одним з вибраних методів: методом ідеальної точки. Для цього визначено перелік альтернативних технологій, які можуть застосовуватись для вирішення задачі та мету, тобто ідеальні параметри мережі, що проектується

та які повинні бути забезпечені при застосуванні визначеної технології. Далі вираховувалась відстань між параметрами кожної з альтернатив та параметрами ідеальної точки. Технологія, яка має мінімальну відстань і вибиралась, як найкраща.

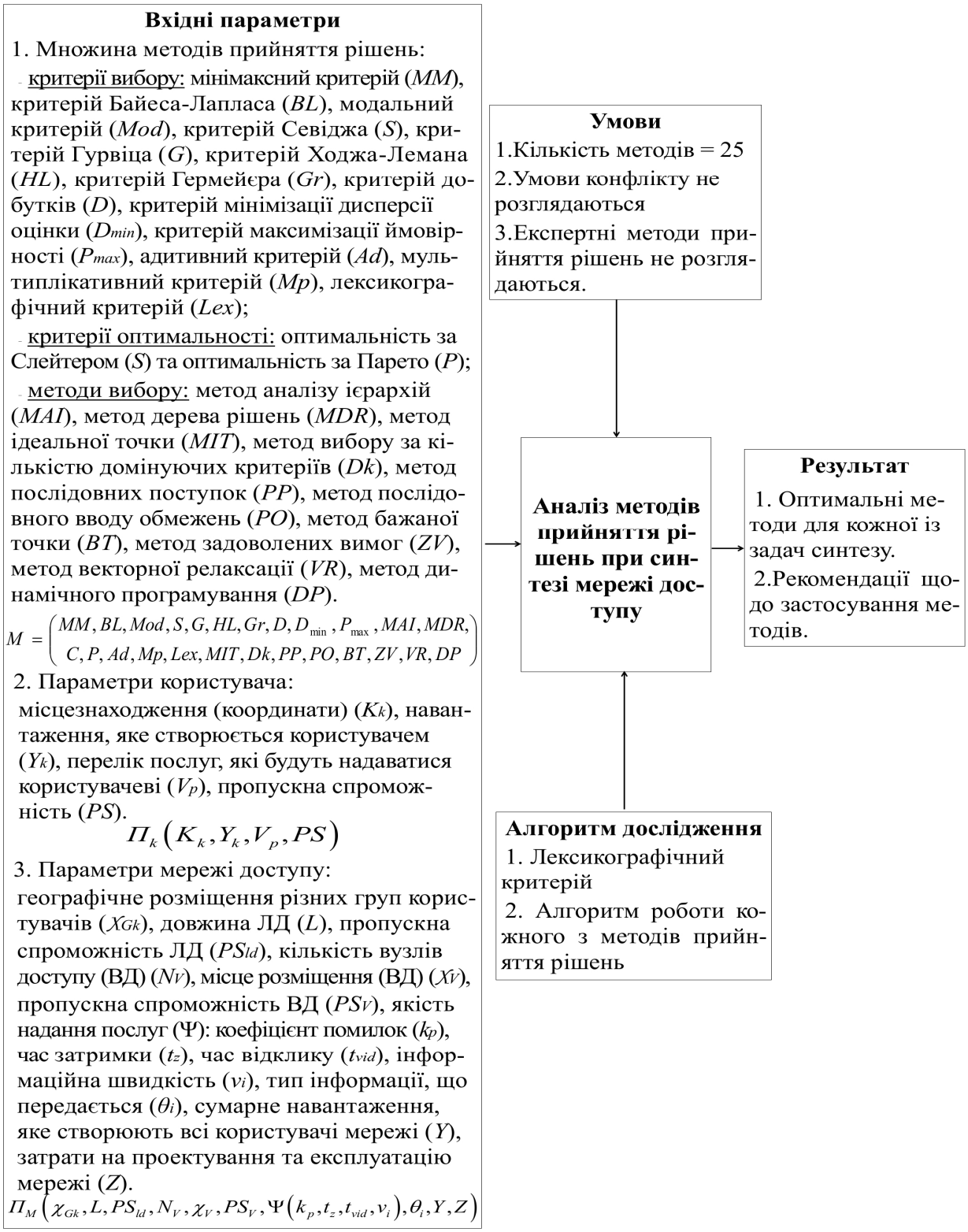


Рис. 1. Модель дослідження.

В дослідженні також проаналізовано використання фіксованого широкосмугового зв'язку для організації мереж доступу та визначено, що

кількість користувачів, які використовують даний вид зв'язку прямо залежить від забезпеченості населення та економічного розвитку країни, чим вищі ці показники тим більше користувачів фіксованого широкосмугового зв'язку. Місце розташування не впливає на кількість підключень до цього виду зв'язку.

В результаті проведення дослідження запропоновано метод удосконалення процесу синтезу мереж доступу шляхом застосування методів теорії прийняття рішень, що дозволяє зменшити трудомісткість цього процесу та долю суб'єктивних суджень дослідника та розроблено рекомендації, щодо застосування методів теорії прийняття рішень для полегшення процесу синтезу мереж доступу та підвищення його ефективності.

Таким чином вперше для вирішення окремих задач синтезу мереж доступу, шляхом вибору за лексикографічним критерієм визначені та обґрунтовані методи теорії прийняття рішень, які доцільно застосовувати для вирішення цих задач.

Дослідження представляє практичну цінність, тому що використання розроблених рекомендації підвищить ефективність процесу синтезу мереж доступу за рахунок зниження трудомісткості вирішення окремих задач. Також, буде знижена доля суб'єктивних суджень дослідника, в процесі синтезу мереж доступу.

Література

1. Дементьев В.Е. Информационно-вычислительные сети : учебное пособие / Дементьев В.Е.– Ульяновск: УлГТУ, 2011. – 141с.
2. Гайворонська Г.С. Мережі та системи абонентського доступу. Частина 1. Технології інформаційних систем. Навчальний посібник / Г.С. Гайворонська – Одеса, 2008. – 379 с.
3. Технотелеком сервіс [Електронний ресурс] // – Режим доступу: *http://www. tts. kiev.ua/?conception NGN* (20.03.15)
4. Офіційний сайт Верховної Ради України [Електронний ресурс] // – Режим доступу: *http://zakon4.rada.gov.ua/laws/show/1280–15* (15.03.15)
5. Бельков В.Н. Автоматизированное проектирование технических систем: Учебное пособие / Бельков В.Н., Ланшаков В.Л. – Москва: "Академия Естествознания", 2009. – 143с.
6. Соломицкий М. Опыт использования методов решения задач выбора в условиях неопределенности и риска при проектировании компьютерных сетей / Соломицкий М., Болотина О. // *Problems of Computer Intellectualization. – Kyiv–Sofia: National Academy of Sciences of Ukraine V.M.Glushkov Institute of Cybernetics, ITHEA*, 2012. – № 28. – P. 318–331
7. Гайворонская Г.С. Задача выбора топологической структуры сети доступа / Г.С. Гайворонская, А.А. Бондаренко // Problems of Computer Intellectualization. – Kyiv–Sofia: National Academy of Sciences of Ukraine V.M.Glushkov Institute of Cybernetics, ITHEA, 2012. – №28 – P.252–261
8. Новікова К.Ю. Вибір засобів апаратно–програмного комплексу обчислювальних мереж на основі нечітких моделей / К.Ю. Новікова // Наукові праці. Комп'ютерні технології. – 2009. – Т.106, №93. – С.127–131.
9. Гайворонська Г.С. Інформаційна мережа, як об'єкт аналізу і синтезу/ Г.С. Гайворонська – Одеса, 2011. – 91 с.
10. Сайт «USICwiki» [Електронний ресурс] // – Режим доступу: http://wiki.usic.org.ua/Динамічне програмування. (15.03.15)
11. Сайт «Библиотека EXSOLVER» [Електронний ресурс] // – Режим доступу: http://exsolver.narod.ru/Books/Mathematic/GameTheory/..(15.03.15)

УДК 004.72

РАЗРАБОТКА МОДЕЛИ СИНТЕЗА СЕТИ ДОСТУПА ПРИ ИСПОЛЬЗОВАНИИ ТЕОРИИ МЕТАПРОЦЕДУР

Гайворонская Г.С., Казак Ю.С.
Институт холода, криотехнологий и экоэнергетики имени В. С. Мартыновского Одесской национальной академии пищевых технологий, Украина
E-mail: flygerl1@bigmir.net

Development model of synthesis of access network of the use of theory meta-procedures

Principles of construction of the access network are already being implemented in the existing telecommunications network, but as not all important nuances of creation of a network of access are worked out up to the end, there are many tasks which need to be decided that promotes to carrying out new researches, comparisons and developments. In research the model of synthesis of a network of access when using the theory of metaprocedures is developed.

Современное состояние телекоммуникационных сетей можно определить термином «движение к совершенству». Вряд ли можно предугадать, как они будут выглядеть в будущем, сколько поколений сетей и технологий предстоит еще пройти. Однако уже сегодня видны первые наработки: мощные сети передач и коммутации пакетов, высокоскоростные линии доступа, оптические телекоммуникационные технологии и т. д., которые и определяют следующие поколения телекоммуникационных сетей.

Сеть доступа (СД) играет важную роль при создании сетей будущего, она является одной из их составляющих, построению которой уделяется много внимания. В течение 20-ти лет с начала предложенной концепции разработки СД разработаны новые методы, позволяющие улучшить показатели ее функционирования, проектирования и внедрения в существующую телекоммуникационную сеть. Это связано с тем, что возможности этих сетей, постоянно расширяясь, выходят на качественно новый уровень и покрывают практически все типы инфокоммуникационных услуг: от передачи голоса и данных до мультимедиа и видео. Различные аспекты построения сетей доступа освещены в работах Соколова Н.А., Гольдштейна Б.С., Бакланова И.Г., Гайворонской Г.С., Ганницкого И.В., Сахаровой С.В., Бондаренко А.А., Котовой А.И. и других. [1…14]

Несмотря на то, что проведено достаточно много исследований, все равно остаются нерешенными ряд задач, к которым можно отнести задачу выбора оптимальной структуры СД. Таким образом, разработка новых рекомендаций, понятийных моделей для решения задачи выбора оптимальной структуры СД поможет решить задачу синтеза СД.

Понятийные модели разрабатываются путем применения прикладных методов теории метапроцедур, которые ранее не применялись при синтезе СД. Метапроцедуры направлены на решение задач интеллектуального типа [15]. В исследовании рассматривается применение метапроцедур, а именно

построение понятийных моделей, в процессе синтеза СД, для выбора наиболее целесообразной структуры сети, анализа всех параметров, которые влияют на построение СД, и определения корреляции между ними.

В ходе проведения исследования, решена задача выбора моделей, пригодных для оптимизации структурных характеристик сети доступа по критерию минимальной стоимости, и при условии обеспечения качества обслуживания, определяемых договором QoS Agreement (SQA) [16]. Результатами исследований являются, понятийная модель проблемы исследования и категориальная модель сети доступа, которые по большинству показателей приемлемости удовлетворяет условиям задачи. Понятийная модель проблемы исследования вида (1) представлена в докладе

$$W_p = \langle W_p, L_p \rangle, \tag{1}$$

где W_p – множество вершин, соответствуют понятиям, которые имеют отношение к проблеме;

L_p – множество дуг, представляющие связи между понятиями.

На ее основе разработана понятийная модель предметной области (2)

$$M_d = \langle W_d, L_d \rangle, \tag{2}$$

где W_d – множество вершин, соответствующих понятие объектной области, к которой относится проблема;

L_d – множество дуг, представляющие связи между понятиями.

Входными параметрами предложенной модели синтеза СД являются, формализованные входные параметры СД, то есть информационные модели для каждого из параметров созданные с помощью формальных языков.

Рис.1. Общая модель синтеза сети доступа.

Основной частью модели синтеза СД при использовании метапроцедур, является блок, в котором содержатся алгоритмы построения понятийных моделей (рис.1). В докладе приведены алгоритмы, отображающие пять правил, которые описывают взаимодействие между введенными понятиями.

Разработанная модель исследования процесса синтеза СД при использовании теории метапроцедур, позволяет рассматривать процесс поэтапно. В свою очередь, это позволило выделить его входные параметры, допущения, критерии, ограничения и условия более детально. Также в ходе исследования разработан алгоритм создания понятийных моделей, отражающий все правила формирования связей в моделях применительно к синтезу СД. Практической ценностью работы является то, что формализация входных параметров СД необходима для создания системы автоматизированного проектирования СД, что упростит процесс синтеза СД.

Литература

1. Соколов Н.А. Развитие сетей доступа и законы Мерфи // Матер. IX Всероссийского научно-технического семинара «Связь в деловой сфере. Новые информационные технологии» / Соколов Н.А // М., 2002.
2. Гольдштейн Б.С. Модернизация сетей доступа в эпоху NGN / Б.С. Гольдштейн, О.П. Орлов, А.Т. Ошев, Н.А. Соколов // Вестник связи. – 2003. – № 60.
3. Гольдштейн Б.С. Цифровизация ГТС и построение мультисервисной сети / Б.С. Гольдштейн, О.П. Орлов, А.Т. Ошев, Н.А. Соколов // Вестник связи. – 2003. – № 4.
4. Соколов Н.А. Семь аспектов развития сетей доступа / Н.А. Соколов // Технологии и средства связи, 2005. – №3. С.1–22.
5. Бакланов И.Г., NGN. Принцыпи построения и организаации, Москва: *Эко-Трендз*, 2008. – с.400.
6. Гайворонская Г. С. Сети и системы абонентского доступа. (Ч 1.) Технологии информационных сетей. Учебное пособие / Г. С. Гайворонская //Одесса: ОГАХ, 2008. – 375 с.
7. Гайворонская Г.С. Структура и функции сетей доступа: Учеб. Пособ. По дисциплине «Системы доступа пользователя» Ч. 1. / Г.С. Гайворонская // Одесса. – ОГАХ. – 2008. – 67 с.
8. Гайворонская Г.С. Уровневая модель сети доступа / Г.С. Гайворонская // Вісник УБЕНТЗ. – №1. – 2004. – Киев. – С. 100-108
9. Гайворонская Г.С. Концепция пользовательского доступа: Учебник для ВУЗов. – Одесса: ОГАХ, 2008. – 408 с.
10. Гайворонская Г.С. Структура и функции сетей доступа: Учеб. Пособ. По дисциплине «Системы доступа пользователя» Ч. 1. – Одесса. – ОГАХ. – 2008. – 67 с.
11. Гайворонская Г.С. Стандартизованные интерфейсы и протоколы доступа: Учеб. Пособ. По дисциплине «Системы доступа пользователя» Ч. 2. – Одесса. – ОГАХ. – 2008. – 48 с.
12. Гайворонская Г.С. Технологии доступа по существующим абонентским линиям. Учеб. Пособ. По дисциплине «Системы доступа пользователя» Ч. 3. – Одесса. – ОГАХ. – 2008. – 90 с.
13. Гайворонская Г.С. Выбор сценария создания СД / Гайворонская Г.С., Сахарова С.В., Котова А.// *Information Technologies & Knowledge: International Journal*, 2012. - №2. – С.143-156
14. Гайворонская Г.С Некоторые задачи модернизации сетей доступа // Г.С. Гайворонская, Ю.К. Корниенко, С.В. Сахарова, Д.А. Юрчук // Материалы IV Международной НТК «Современные информационно-коммуникационные технологии»: Збірник тез. К. – ДУІКТ. – 2008. – С.34.
15. Гладун В.П., Партнерство с комп`ютером. Человеко-машинные целеустремленные системы, Київ: Port Royal, 2000 – 116 с.
16. Технології та середовища зв’язку [Електронний ресурс] // – Режим доступу: http://www.rmmc26205.ru/soglashenie (01.12.2014р.).

УДК 004.713

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ОПТИЧЕСКИХ ПРОЦЕССОРОВ ДЛЯ УПРАВЛЕНИЯ КОММУТАЦИЕЙ ОПТИЧЕСКИХ СИГНАЛОВ

Гайворонская Г.С., Рыбалов Б.А.
Институт холода, криотехнологий и экоэнергетики имени В. С. Мартыновского, ОНАПТ, Украина
E-mail: ikt.osar@gmail.com

Investigation of the possibility of using optical processors to control the switching of optical signals

The feasibility of using optical processors in all-optical networks is evaluated in this paper. The model of all-optical switching device is examined. Were suggested an optical processors, which are the most promising in the field of optical technologies.

Анализ источников, посвященных созданию оптических сетей [1-4] показал, что на данный момент вопросы, относящиеся к функционированию волоконно-оптических систем передачи, изучены достаточно хорошо. В то же время вопросы реализации оптических систем коммутации рассмотрены поверхностно и требуют проведения дальнейших исследований. В настоящее время существуют лишь общие концептуальные подходы к построению оптических коммутаторов, требующие развития и тщательного исследования. Для осуществления этого исследования необходимо разработать модель полностью оптического коммутатора, который будет не только коммутировать сигналы в оптической форме, но и обеспечит управление процессом коммутации с помощью оптического излучения. Некоторые аспекты этой задачи рассмотрены в работах [5-8], однако в этих работах авторами рассмотрены лишь подходы к решению задачи управления коммутацией оптических сигналов, которые не позволили получить приемлемого результата. Поэтому принято решение рассмотреть возможность использования оптических процессоров, которые уже хорошо зарекомендовали себя при решении задач матричного умножения, распознавания образов, квантовых вычислений, обработки изображений.

Первоначально основным элементом оптических компьютеров являлся жидкокристаллический пространственный модулятор, на заднюю поверхность которого был нанесен фотопроводник. При падении света на фотопроводник локально изменяется потенциал, воздействующий на жидкий кристалл и приводящий к изменению пропускания светового потока элемента. Используя управляющий луч с одной стороны устройства и считывающий луч с другой стороны, возможно создание бистабильного логического элемента и реализация булевской логики. В бистабильных логических элементах контролируемым параметром является интенсивность света на входе в систему, а два устойчивых состояния соответствуют двум значениям интенсивности света на ее выходе. Следует отметить, что

быстродействие данного устройства определялось инерционностью жидкого кристалла.

В конце 90-х годов прошлого века велись работы по созданию оптического компьютера с логической матрично-тензорной основой [9]. В устройстве планировалось использовать входную матрицу лазеров, соединенную планарными волноводами и обычной оптикой с матрицами переключения, на основе дифракционных оптических элементов, и выходную систему, состоящую из матрицы лавинных фотодиодов, совмещенную с матрицей вертикально-излучающих диодов. Фирма Opticomp Corporation разработала новый интегральный оптический элемент, состоящий из матрицы VCSEL лазеров и фотодетекторов, соединенных волноводом, и использует эти устройства, как для обработки информации, так и для создания сверхбыстрых переключателей в сверхплотных волоконных линиях связи [10].

В данной работе сделана попытка оценить целесообразность использования оптических процессоров и определить условия их применения для управления процессом коммутации оптических сигналов. Объектом исследования является полностью оптическое коммутационное устройство, предметом – методы управления коммутацией оптических сигналов. Цель работы: повышение быстродействия полностью оптических сетей.

Задача исследования: разработка модели и методов реализации полностью оптической коммутации, не использующих электронно-оптического и оптоэлектронного преобразования информационного сигнала и не требующих буферизации оптического сигнала в полностью оптическом коммутационном устройстве (ПОКУ).

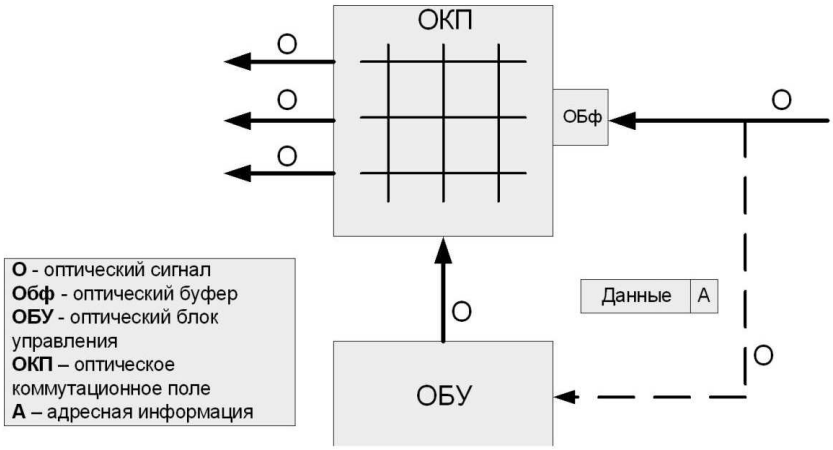


Рис.1. Структурная схема полностью оптического коммутационного устройства.

В такой модели (рис.1) информационный оптический сигнал, переносящий некоторый блок информации, одновременно запоминается в оптическом буфере (ОБф) и поступает на вход оптического блока управления (ОБУ). Оптический блок управления выполняет анализ информационного блока, выделяет адресную информацию и после ее обработки генерирует оптический сигнал управления оптическим коммутационным полем (ОКП).

Затем оптический сигнал извлекается из ОБф и следуя по коммутационному пути поступает на выход, и после усиления мощности сигнал передается по оптическому волноводу.

Несмотря на всю привлекательность полнооптического подхода к построению коммутационных устройств, его применение в настоящий момент вызывает ряд сложностей. В первую очередь, это касается реализации ОБУ, использующего оптические процессоры, которые имеют сегодня ограниченное применение из-за высокой стоимости.

К преимуществам оптических технологий для современных оптических процессоров можно отнести:

- принципиальное повышение производительности;
- возможное уменьшение размеров элементов схем;
- снижение потребляемой мощности;
- пониженное тепловыделение.

Для реализации оптических процессоров для полностью оптических сетей предлагается использовать оптические процессоры, основанные на методах теории нечетких множеств, а также оптические процессоры, совмещенные с голографическими запоминающими устройствами, так как эти процессоры представляются наиболее перспективными в области оптических технологий. Некоторым результатам выполненных исследований посвящен предлагаемый доклад.

Литература

1. Оптика наноструктур. Под редакцией А. В. Федорова: СПб. «Недра», 2005 г.
2. Гайворонская Г.С. Коммутаторы оптических сигналов / Г.С. Гайворонская, А.В. Рябцов // Холодильна техніка і технологія. – Одеса. – 2009. – №2 (118). – С.55-59.
3. Guilfoyle P.S., McCallum D.S. High-speed low-energy digital optical processors. // Optical Engineering, 1996, V. 35, P. A3-A9.
4. Arestova M.L., Bykovsky A.Yu. Possibilities for Optoelectronic Parallel Image Processing Based on Principles of Multiple-Valued Logic. // Photonics and Optoelectronics, 1994, v.2, i.4, pp.169-180.
5. Gayvoronska G.S. Features of optical switches' usage in the modern information networks / G.S. Gayvoronska, A.V. Ryabtsov // Applicable Information Models. – Sofia: ITHEA, 2011. – № 22. – P. 169-181.
6. Гайворонская Г.С. Проблема обеспечения полностью оптической коммутации в конвергентных сетях / Г.С. Гайворонская // Збірник тез V МНТК «Проблеми телекомунікацій». – Київ. – НТУУ «КПІ». – 2011. – С.39
7. Гайворонская Г.С. Анализ возможности использования феноменологической модели оптической системы коммутации при построении полностью оптических сетей/ Г.С. Гайворонская, А.В. Рябцов//Збірник материалов VI МНТК «Проблеми телекомунікацій».– Київ.– НТУУ «КПІ».– 2012.– С.99
8. Гайворонская Г.С. Оценка корректности применения метода раздельных потерь для определения структурных параметров оптических систем коммутации / Г.С Гайворонская, А.В. Рябцов, И.В. Ганницкий // Холодильна техніка і технологія. – Одеса. – ОДАХ, 2012. – № 5 (139) – С. 84-88
9. Арестова М.Л., Быковский А.Ю. Методика реализации оптоэлектронных схем многопараметрической обработки сигналов на основе принципов многозначной логики // Кв. Электр., 1995, т.22, в.10, с.980-984.
10. Guilfoyle P.S., Rudokas R.S., Stone R.V., Roos E.V. Digital optical computer II: performance specifications. // Optical Computing Technical Digest, 1991, P. 203-206.

УДК 621.395

РОЗРАХУНОК ПОКАЗНИКІВ ЯКОСТІ КАТЕГОРІЙНОГО ОБСЛУГОВУВАННЯ ЗАЯВОК ПРИ АБСОЛЮТНОМУ ПРІОРИТЕТІ НА ІНТЕЛЕКТУАЛЬНІЙ МЕРЕЖІ ЗВ'ЯЗКУ

Правило В.В.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: valeriy_pravilo@ukr.net

Calculation service of category quality applications to the absolute priority to intellectual communication network

Considering calculation service of category quality applications to the absolute priority. Expressions quoted in the article to take into account the stage of design intelligent network, which further losses appear on the network using subscribers category. Was designated the algorithm applications service with absolute priority.

Будь-яка заявка, що надійшла в мережу в момент наявності в ній хоча б одного вільного каналу, що відповідає технічним вимогам, займає цей канал і вважається на даному етапі виконаною. Встановленому в такий спосіб з'єднанню при категорійному обслуговуванні надається певна категорія.

Рівень категорії, що надається з'єднанню, залежить від різних об'єктивних і суб'єктивних факторів. В „класичному" випадку з'єднанню надається вища категорія з категорій користувачів, що беруть участь в цьому з'єднанні.

При визначенні показників якості пріоритетного обслуговування заявок повинен бути визначений повний перелік вихідних даних, у тому числі і алгоритм встановлення з'єднання, особливо у випадках зайнятості всіх каналів в гілках напрямку зв'язку або в групі обслуговуючих приладів необхідної служби центру інтелектуальних послуг (ЦІП).

Перелік вихідних даних не залежно від виду пріоритетного обслуговування включає:

- число категорій заявок n;
- вид потоків заявок кожної категорії (найпростіший, примітивний);
- інтенсивність навантаження, що створене потоками заявок кожної категорії ρ_i;
- прогнозоване значення інтенсивності виконаного навантаження, що обумовлене викликами абонентів нижчих категорій абонентами вищих категорій $\rho_j^{(i)}$ ($j=1…n$, $i=2…n$). При цьому службам ЦІП категорії пріоритету можуть надаватися по тим самим ознакам, що і іншим користувачам (абонентам) інтелектуальної мережі спеціального призначення;
- число каналів у гілці ІМСП (обслуговуючих приладів у службі ЦІП) V.

Розглянемо алгоритм обслуговування заявки на встановлення з'єднання при відсутності вільних каналів (обслуговуючих приладів) у необхідному напрямку зв'язку:

А1 − на гілку ІМСП надходить заявка *і-оїї* категорії;

Р2 − здійснюється перевірка наявності в гілці вільних каналів, тобто

перевіряється умова: чи є в даній гілці хоча б один вільний канал?

А3 − рішення: вільних каналів у момент надходження заявки на обслуговування в гілці немає;

Р4 – перевіряється умова: чи є в даній гілці з'єднання з категорією нижче *і-оїї*;

А5 − у даній гілці з'єднання з категорією нижче *і-оїї* є;

А6 − обирається канал, що перебуває в з'єднанні найнижчої категорії;

А7 − дається команда на роз'єднання даного з'єднання (практично роз'єднання відбувається після подачі сигналу про пріоритетне скидання користувачам, що знаходяться в даному з'єднанні);

А8 – канал, що звільнився, займається для обслуговування *і-оїї* заявки;

А9 (після Р4) − в даній гілці з'єднання з категорією нижче *і-оїї* немає;

А10 − заявка, що надійшла, одержує відмову й вибуває із системи обслуговування.

Мовою логічного системного алгоритму (ЛСА) цей алгоритм має вигляд:

$$\boldsymbol{A1\ P2\ A3\ P4}\overset{5}{\uparrow\downarrow}_{9}\ \boldsymbol{A5\ A6\ A7\ A8}\ {}^{4}\boldsymbol{A9\ A10\ K.}$$

Як випливає з наведеного алгоритму, у розглянутому випадку заявки (і встановлені по них з'єднання) піддані двом видам втрат:

- втрати через зайнятість каналів (обслуговуючих приладів);
- втрати через „пріоритетне скидання".

Слід зазначити, що випадкові події, які обумовлюють ці втрати, є несумісними. Якщо заявка загублена через зайнятість каналів, то зрозуміло, що пріоритетного скидання не буде. Якщо з'єднання розірване через пріоритетне скидання, то так само очевидно, що заявка раніше була обслужена й не губилася. У зв'язку із цим, повна ймовірність одержати відмову p може бути отримана як арифметична сума ймовірностей зазначених подій:

$$p = p_i + p_{0i}, \tag{1}$$

де: p_i – імовірність втрат заявки *і-оїї* категорії через зайнятість всіх каналів (обслуговуючих приладів);

p_{0i} − імовірність втрат заявки *і-оїї* категорії через „пріоритетне скидання".

Відповідно до визначення абсолютного пріоритету втрати заявок від споживачів вищої категорії через зайнятість каналів (обслуговуючих приладів) визначаються тільки навантаженням від споживачів цієї категорії й числа каналів (приладів). З огляду на те, що вищий пріоритет може надаватися обмеженій групі споживачів інтелектуальних послуг (у противному випадку таке категорування втрачає зміст), розрахунок імовірності втрат для заявок цієї групи варто робити по методу Енгсета, тобто:

$$p_c = \frac{C_{S-1}^{V}(kt)^{V}[1-(kt)]^{S-V}}{\sum_{i=0}^{V} C_{S}^{i}(kt)^{i}[1-(kt)]^{S-i}}, \tag{2}$$

де: p_c – імовірність втрат по викликах;

C_{S-1}^{V} - число сполучень із S-1 по V;

S – кількість користувачів конкретного виду послуг;

V – кількість каналів, що забезпечують доступ до послуги;

kt – інтенсивність навантаження, що надходить від одного джерела заявок вищої категорії й виконаної за заявками від джерел інших категорій до споживача даної категорії.

Для користувачів нижчої (n) категорії ймовірність втрати заявки через зайнятість всіх каналів (обслуговуючих приладів) може бути визначена по першій формулі Ерланга, з урахуванням навантаження, що надходить на цю гілку від користувачів всіх категорій:

$$p_n = \frac{\left(\sum_{j=1}^{n} \rho_j\right)^V}{V!} \left[\sum_{K=1}^{V} \left(\sum_{j=1}^{n} \rho_j\right)^k / k!\right]^{-1}. \qquad (3)$$

У загальному випадку ймовірність одержати відмову в обслуговуванні заявки *i-ої* категорії через зайнятість каналів у гілці (обслуговуючих приладів у ЦІП) визначається за першою формулою Эрланга при навантаженні ρ*, де:

$$\rho^* = \sum_{j=1}^{i} \rho_j + \sum_{j=1}^{i} \rho_j^{(n)} (1 - p_n) + \sum_{j=1}^{i} \rho_j^{(n-1)} (1 - p_{n-1}) + \ldots + \sum_{j=1}^{i} \rho_j^{(i+1)}. \qquad (4)$$

По визначенню абсолютного пріоритету ймовірність втрат заявок вищої категорії від пріоритетного скидання відсутня, тобто $p_{01} = 0$. Значення ймовірності втрат заявок цього типу для нижчої (n-ої) категорії може бути отримане відповідно до визначення як:

$$p_{0n} = \sum_{j=1}^{n-1} \rho_j (p_n - p_{n-1}) / \rho_n (1 - p_n),$$

де: у чисельнику показане значення інтенсивності додаткового навантаження, створюваного заявками 1 ... (n - 1)-х категорій.

На основі подібних міркувань імовірність втрат заявки довільної (крім вищої) категорії може бути визначена з виразу:

$$p_{0i} = \sum_{j=1}^{i-1} \rho_j (p_i - p_{i-1}) / \rho_i (1 - p_i),$$

Пам’ятаючи про несумісність розглянутих подій: втрат заявок через зайнятість каналів, і через пріоритетне скидання, розрахунок їх ймовірностей робиться незалежно.

Література

1. *Галкин В.А., Григорьев Ю.А.* Телекоммуникационные сети. – М.: МГТУ, 2003. – 341 с.
2. *Гольдштейн Б.С., Ехриель И.М., Рерле Р.Д.* Интеллектуальные сети. – М.: Радио и связь, 2000. – 432 с.
3. *Крестьяников С.В., Полканов Е.М., Шнепс-Шнеппе М.А.* Интеллектуальные сети и компьютерная телефония // Радио и связь, 2001. - № 11. – С. 24 − 28.
4. *Башарин Г.П., Харкевич А.Д., Шнейс М.А.* Массовое обслуживание в телефонии. – М.: Наука, 1968. – 214 с.

УДК 621.395

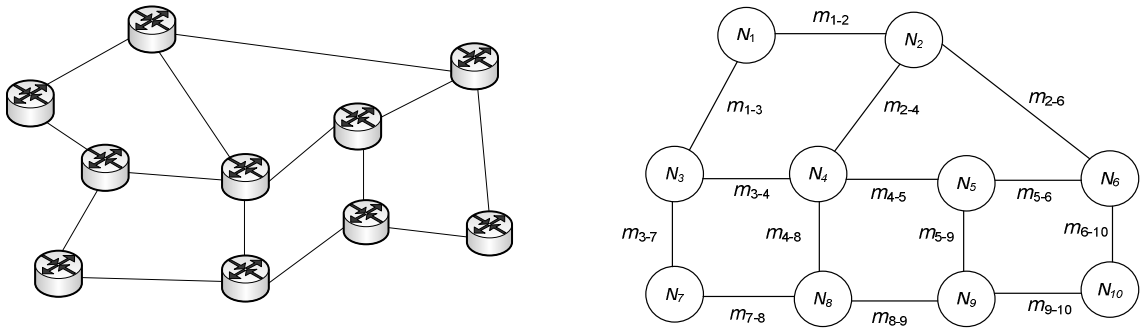
СИНТЕЗ РАЦІОНАЛЬНОЇ СТРУКТУРИ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ ЗА ЗАДАНИМИ ПОКАЗНИКАМИ

Правило В.В.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: valeriy_pravilo@ukr.net

Synthesis of rational telecommunications network for a given indicators

Presented the synthesis technique of structure of the telecommunication network in terms of cost and minimum structural reliability using heuristic search algorithms. Presented a block diagram of the algorithm technique.

Під синтезом структури телекомунікаційної мережі (ТКМ) розуміється визначення кількості комутаційних центрів (КЦ), місць їхнього розгортання, а також параметри ліній між ними. Структуру, що враховує місця розгортання вузлів і ліній зв'язку на місцевості, прийнято називати топологічною [1]. Дуже часто для синтезу структури мережі її представляють у вигляді графу *G(N,M)*, де *N* – кількість вершин (КЦ), *M* – кількість ребер (гілок). Приклад варіанту телекомунікаційної мережі і відповідного їй графу показано на рис. 1.



а) б)

Рис 1. Подання структури ТКМ у вигляді графу:
а – варіант побудови структури ТКМ;
б – відповідний даній ТКМ граф.

Рішення задачі синтезу раціональної топологічної структури ТКМ, по своїй суті, складається в рішенні завдання знаходження різних раціональних первісних топологічних структур і вибору прийнятного результату з отриманої безлічі рішень.

Можна виділити два класи алгоритмів для рішення завдань синтезу мережі зв'язку [3]:

- алгоритми суворої оптимізації;
- алгоритми евристичного пошуку.

До числа алгоритмів суворої оптимізації відносяться алгоритми, що використовують метод цілочисленого лінійного програмування й метод гілок і границь [4]. Дані алгоритми мають наступні недоліки:

- у більшості випадків, істотні витрати машинного часу не дозволяють знайти раціональне рішення;

- не завжди можливо коректно описати нелінійні обмеження існуючих систем за допомогою лінійних співвідношень, що приводить до похибки одержуваних результатів;
- у ряді випадків у процесі рішення завдання необхідно змінити обмеження, що не завжди можливо.

Найбільше розповсюдження одержали евристичні алгоритми, які в умовах обмеження часу дозволяють при покроковій зміні заданої первісної структури мережі, одержати вузький діапазон структур, що задовольняють заданим вимогам.

На сьогодні відома досить велика кількість алгоритмів, створених для рішення проблем проектування багатовузлових мереж. Основні з них це – алгоритми Краскала, Єжі-Віл'ямса, Фогеля, Шарма та ін.

Розглянуті евристичні алгоритми синтезу початкових структур ведуть до одного із припустимих рішень. Однак знайдене рішення не може бути поліпшено цим же алгоритмом, незалежно від того яким далеким є це рішення від раціонального. Дослідження показують, що алгоритм Краскала найбільш простий у реалізації й працює краще інших. Він дозволяє одержувати субраціональні рішення й забезпечує можливість послідовно наближатися до раціонального рішення. З огляду на вищесказане, пропонується доцільним використати алгоритм Краскала для первісного синтезу структури мережі.

Для подальшого поліпшення синтезованої за допомогою евристичного алгоритму Краскала початкової структури ТКМ, з метою одержання раціональної за вартістю й структурною надійністю кінцевої структури, необхідно застосувати один з методів синтезу топологічних структур ТКМ, що носять евристичний характер (метод Стейглиця, метод заміни гілок, метод видалення гілок, метод насиченого перетину). Для одержання раціональної структури мережі на основі синтезованої початкової структури доцільно застосовувати метод насиченого перетину, як найбільш простий у реалізації і який дає можливість включення в мережу позначених потрібних ребер.

Завдання синтезу раціональної топологічної структури ТКМ у загальному вигляді можуть бути сформульовані в такий спосіб: спроектувати раціональну структуру ТКМ ($A=\{a_{ij}\}$), мінімізовану за вартістю ($\min C$, де C – сумарна вартість мережі зв'язку), і забезпечити задані показники структурної надійності ТКМ ($W_{ij}^{\text{н}}$ або $W_{\text{ткм}}^{\text{н}}$). Методика синтезу ТКМ повинна відповідати наступним умовам:

- випадковому характеру взаємного розміщення заданих КЦ;
- обмеженістю часу на ухвалення рішення про будівництво або розгортання ТКМ;
- заданим обмеженням про наявність сил і засобів для будівництва ліній зв'язку, наведеним до максимально можливої кількості ліній зв'язку ($L_{\max}$) і їхніх довжин (l_i^{max}, де l_i – довжина i-ої лінії зв'язку, $i=\overline{1,L_{\max}}$).

У такій постановці формально задачу синтезу ТКМ можна записати в наступному вигляді:

$$F=\{a_{ij}\},\Leftrightarrow minC/W_{ij}\geq W_{ij}^{\text{н}};$$

$$L\leq L_{\max};$$

$$l_i\leq l_i^{max},\quad i=\overline{1,L_{\max}}.$$

Вихідними даними для синтезу ТКМ будуть:

- задані показники структурної надійності ТКМ у вигляді матриці $\left|W^{\text{Н}}\right|$, елементами якої є задані показники структурної надійності всіх напрямків зв'язку $W_{ij}^{\text{н}}$ й заданий (нормований) показник структурної надійності ТКМ у цілому $W_{\text{ТКМ}}^{\text{Н}}$;

- необхідна кількість КЦ N, з координатами їхнього розміщення (x_i, y_i);

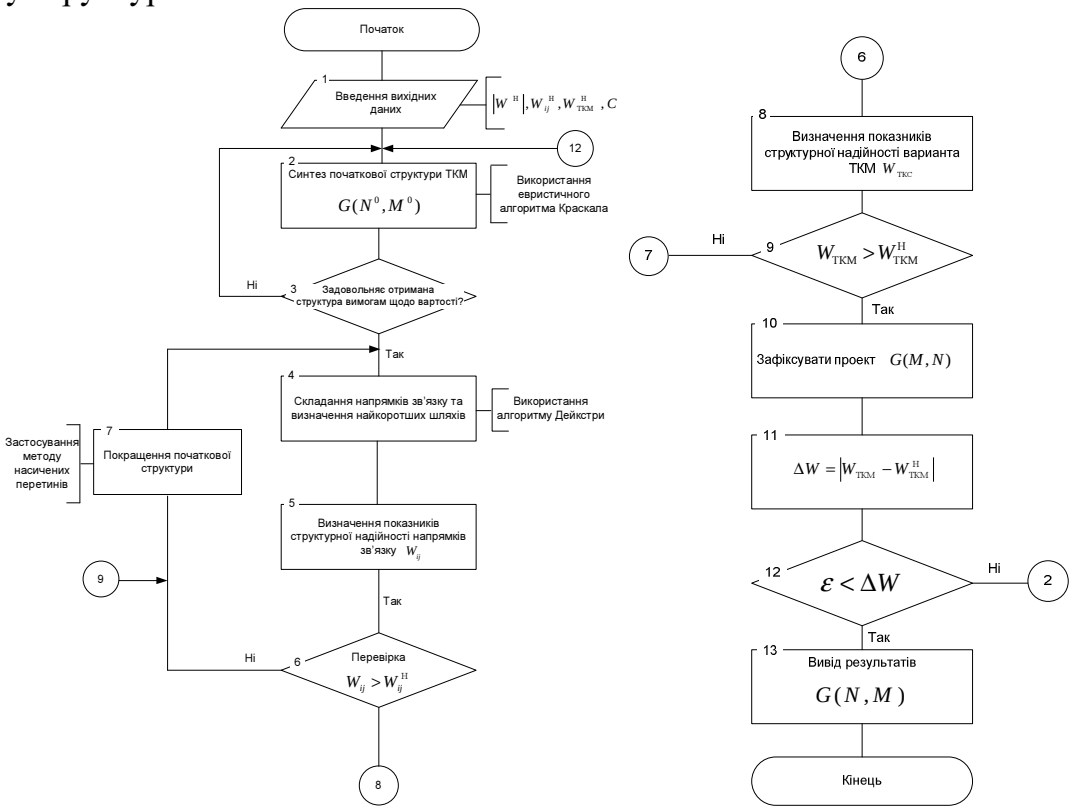
- наявність сил і засобів для будівництва ліній зв'язку ($L_{\max}$ і l_i^{max}).

У результаті проведених розрахунків визначаються:

- раціональна структура ТКМ для забезпечення необхідних показників структурної надійності ТКМ, задана матрицею зв'язаності $\left|A\right| = \left\{a_{ij}\right\}$ або графом $G(N, M)$;

- реальні значення показників структурної надійності всіх напрямків зв'язку ТКМ, представлені у вигляді матриці $\left|W\right| = \left\{W_{ij}\right\}$ й показник структурної надійності ТКМ $W_{\text{ТКМ}}$.

Представлено блок-схему алгоритму, що реалізує запропоновану методику синтезу структури ТКМ.



Література

1. Кутузов О.И. Татарникова Т.М. Моделирование телекоммуникационных сетей. – С.-П.: СПГУТ, 2005, – 80 с.
2. Романов А.И. Телекоммуникационные сети и управление. – К.: ИПЦ „Киевский университет", 2003. – 247 с.
3. Романов О.І., Правило В.В. Дослідження впливу параметрів функціонування гілки телекомунікаційної мережі на показник якості обслуговування заявок. // Збірник наукових праць ВІТІ НТУУ "КПІ", Випуск № 2, 2006. – С. 75–80.
4. Мизин И.А., Богатырев В.А., Кулешов А.П. Сети коммутации пакетов / Под ред. В.С. Семенихина. – М.: Радио и связь, 1986. – 408 с.

УДК 621.3

ОЦІНКА ПРОПУСКНОЇ СПРОМОЖНОСТІ SHDSL-СИСТЕМИ ПЕРЕДАЧІ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ EFM

Куляс А.А., Носков В.І.
Інститут телекомунікаційних систем НТУУ «КПІ»
E-mail: kulyas.ann32@gtmail.com

Evaluation of capacity for SHDSL-transmission system using the technology of EFM

This article deals with analyses of the capacity for SHDSL-transmission system using the technology of EFM. Conclusions were made based on practical results and theoretical calculations according to network structure.

У сучасних телекомунікаційних мережах, а саме на ділянці доступу, поширена технологія EFM (Ethernet in the First Mile – Ethernet на першій милі), яка забезпечує практично прозору передачу Ethernet-кадрів з додаванням функції моніторингу якості їх передачі (функція OAM – Operation, Administration and Maintenance). Існує три різновиди стандарту EFM: доступ по мідним лініям (2Base-TL, 10PASS-TS); доступ по активним оптоволоконним лініям (100BASE-LX10, 100BASE-BX10, 1000BASE-LX10, 1000BASE-BX10); доступ по пасивним оптоволоконним лініям (1000BASE-PX10, 1000BASE-PX20, 1000BASE-PX30, 1000BASE-PX40).

Метою досліджень є оцінка пропускної спроможності обладнання, побудованого згідно стандарту EFM2Base-TL (IEEE 802.3, section 5), який у частині формування та обробки лінійного сигналу базується на стандарті SHDSL (MCE-T G.991.2).

Оцінка проводилась як для однопарного режиму, де є мінімальні відмінності від стандарту SHDSL, так і для багатопарного режиму, де використовується принцип агрегації трафіку різних пар - PAF (PME Aggregation Function).

Оцінка має дві складові. По-перше, це теоретичні розрахунки коефіцієнту використання пропускної спроможності лінійного тракту SHDSL у залежності від довжини UDP пакету, який, в свою чергу, залежить від виду трафіку (данні, голос, тощо). По-друге, це практичні дослідження пропускної спроможності SHDSL-лінії, побудованої на обладнанні Watson EFM (виробник компанія Schmid Telecom, Швейцарія).

Теоретичні розрахунки базувались на аналізі співвідношення службових полів та полів корисного навантаження фреймів стеку протоколів

та методів перетворень, які використовуються в ланцюгу передачі сигналів користувачів - від Ethernet- кадрів до безпосередньо лінійного сигналу TC-PAM. При цьому особливий інтерес був у дослідженні впливу техніки агрегації/розподілу Ethernet-трафіку з різних пар кабелю, яка використовується в стандарті 2Base-TL та носить назву PAF. Принцип PAF показано на рис.1.

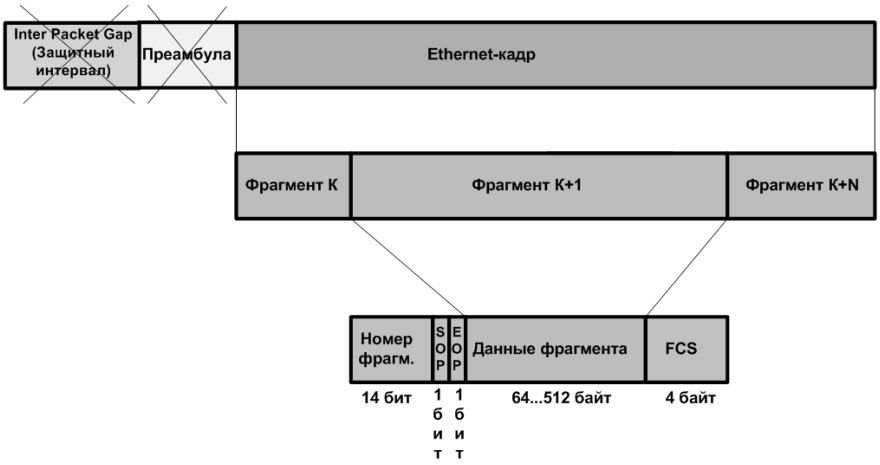


Рисунок 1. Принцип PAF

Процедура PAF включає в себе сегментацію кадрів Ethernet на фрагменти з додаванням номерів фрагментів та деяких службових полів і подальшу передачу фрагментів за технологією SHDSL по різним парам кабелю. На протилежній стороні лінії відбувається відтворення повного Ethernet-кадру за номерами фрагментів. Так як при цій процедурі мають місце додавання службових даних, то це має знижувати коефіцієнт використання пропускної спроможності SHDSL-лінії. Окрім того, на цей коефіцієнт буде впливати і довжина кадру Ethernet, яка залежить від виду трафіку, що передається. Результати розрахунків наведені у табл. 1.

Таблиця 1.

Вид трафіку	*Довжина UDP/TCP пакету*	*Довжина кадру Ethernet*	*Коефіцієнт використання пропускної спроможності*		
			1 пара	*2 пари*	*4 пари*
VoIP	~58	~76	0,511	0,459	0,414
Web(HTTP)	>1500	1518	0,948	0,941	0,934
FTP	>1500	1518	0,948	0,941	0,934

Для практичних досліджень коефіцієнта використання пропускної спроможності була побудована натуральна модель SHDSL-лінії з

використанням обладнання Watson EFM (SZ.868.V654). У якості інструменту для вимірів використовувалась програма генерації трафіку та аналізу пропускної спроможності JPERF 2.0.2, а також програма BT (Bandwidth Tester) від компанії Mikrotik. Результати вимірів наведені у табл.2.

Таблиця 2

Довжина UDP/TCP пакету	Довжина кадру Ethernet	Коефіцієнт використання перепускної спроможності		
		1 пара	2 пари	4 пари
58	76	0.48	0.39	0.3789
1500	1518	0.90625	0.8906	0.8789
1500	1518	0.90625	0.8906	0.8789

Висновки:

1. Техніка агрегації трафіку різних пар, яка використовується у стандарті EFM 2Base-TL, призводить до зниження коефіцієнта використання перепускної спроможності у порівнянні з однопарним режимом на 1,5…10 відсотків у залежності від кількості пар та виду трафіку

2. Найнижчий коефіцієнт використання перепускної спроможності спостерігається для коротких кадрів Ethernet, які характерні для VoIP. Це пояснюється зменшенням корисних полів пакетів протоколів по відношенню до фіксованих службових полів

3. Розбіжність між теоретичною оцінкої та даними практичних досліджень знаходиться у межах 3…6 відсотків

Література

1. RFC 791.

2. RFC 793.

3. RFC 768.

4. IEEE P802.3ah Ethernet in the First Mile Task Force.

5. Носков В.І. WatsonEFMPlug-in Техническое описание и руководство по эксплуатации 2012- 43с.

6. Олифер В. Г., Олифер Н. А. Глава 13. Коммутируемые сети Ethernet // Компьютерные сети. Принципы, технологии, протоколы. — 4-е изд. — СПб.:Питер, 2010. — С. 438.

УДК 621.391

КЛАСИФІКАЦІЯ ПРОТОКОЛІВ MAC РІВНЯ ДЛЯ AD-HOC МЕРЕЖ

Максимов В.В., Литвин О.О.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: litvinolek@gmail.com

Classifications of MAC protocols for Ad-Hoc networks

Due to technological advances for ad-hoc networks created many Medium Access Control (MAC) layer protocols. In this paper, we classify these protocols. Five key features emerging: contention-based protocols, with reservation, with scheduling, with routing management, with power and directions management. Also, our classification focuses categorizing protocols which resolve hidden and exposed terminal problem.

Управління доступом до середовища (Medium Access Control (MAC)) – це підрівень канального рівня моделі OSI. У бездротових ad-hoc мережах, враховуючи обмежений спектр, змінні в часі характеристики поширення, розподілений контроль доступу і енергетичні обмеження, виникає багато проблем для можливості створення «ефективного» MAC протоколу та забезпечення надійного зв'язку із високою швидкістю передавання даних. Одними з основних виступають проблеми прихованих та незахищених вузлів (рис.1).

Під проблемою прихованого вузла розуміється колізія через одночасне передавання вузлами, які мають між собою двоскачковий зв'язок, пакетів до їх спільного односкачкового сусіда. Проблема незахищеного вузла – нездатність вузла здійснювати передавання іншим вузлам через здійснення передавання своїм сусідом.

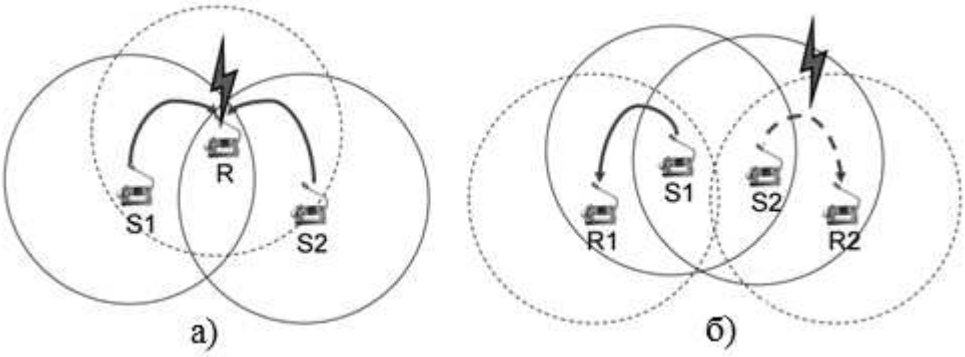


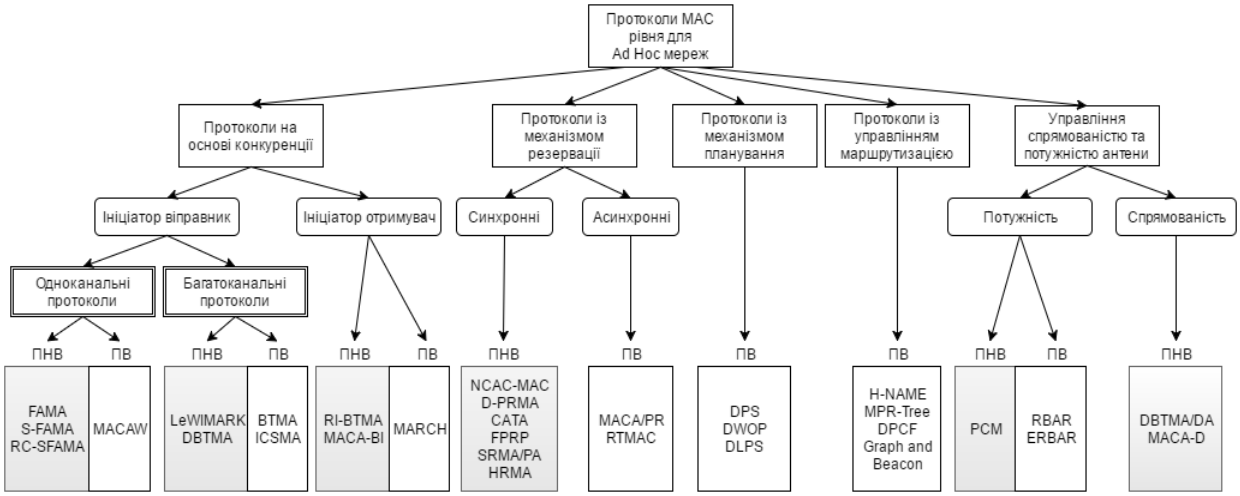
Рис. 1 Проблеми прихованих вузлів (а) та незахищених вузлів (б).

В результаті досліджень, з метою створення такого протоколу, на даний момент існує велика кількість MAC протоколів, кожен з яких має свої переваги та недоліки. Тому дуже важливу роль відіграє осмислене впорядкування протоколів за певними ознаками, тобто створення класифікації. У [1-7] запропоновано найбільш типові варіанти класифікації:

Так у класифікації, запропонованій в [1], протоколи поділяються за наступними 6-ма ключовими ознаками: розподілення каналів і доступу, топологія, потужність, ініціація передавання, дальність дії, завантаження мережі і масштабування. Класифікація, що запропонована в [2], враховує лише діаграми спрямованості антен. Ключовою ознакою виступає спосіб доступу до каналу, який

може бути випадковий чи синхронізований. Протоколи із випадковим доступом у свою чергу поділяються на ті, що використовують контрольні RTS/CTS пакети і ті що використовують тони зайнятості. Варіант класифікації, запропонований у [3], характеризує різні аспекти роботи протоколів і поділяє їх на 3 категорії (із рукостисканням, управлінням маршрутизацією, використанням тонів зайнятості). З іншого боку, вони також розподілені по часу винайдення та відображені генеалогічні корені їх виникнення. У [4-7] відображено кілька версій класифікації, яка має спільні критерії та структуру, але відрізняється кількістю протоколів які до неї входять. У ній протоколи поділяються за способом доступу до каналу: на основі конкуренції (вільного доступу), із механізмом резервації, планування, та інші.

В даній роботі запропонована класифікація, в основу якої лягла запропонована в [4-7], але із урахуванням особливостей, вище перерахованих в [1-3]. Основний акцент зроблено на здатність протоколів вирішувати проблеми прихованих та незахищених вузлів (рис. 2).



ПНВ – вирішення проблеми прихованих та незахищених вузлів
ПВ – вирішення проблеми прихованих вузлів

Рис. 2. Класифікація протоколів MAC рівня для Ad-Hoc мереж

В дану класифікацію ввійшли: протоколи на основі конкуренції, із механізмом резервації, із механізмом планування, із управлінням маршрутизацією, із управлінням потужністю та спрямованістю. Для протоколів на основі конкуренції характерна відсутність резервування ресурсів, а кожного разу, перед передаванням пакету вузол узгоджує із сусідами доступ до сумісно використовуваного каналу. Дані протоколи поділяються за ознакою ініціації передавання на протоколи із ініціатором відправником та отримувачем. Протоколи, в яких ініціатором виступає відправник, поділяються на одноканальні, в яких вся ширина смуги пропускання використовується як одне ціле, та багатоканальні, в яких ширина смуги пропускання поділяється на кілька каналів, що дозволяє підтримувати одночасне передавання кількома вузлами, та розділяти по різних каналах передавання службових та інформаційних пакетів. До одноканальних протоколів, в яких вирішується ПНВ ввійшли: FAMA, S-FAMA, RC-SFAMA. Серед багатоканальних проблему ПНВ вирішують протоколи Le-WIMARK та DBTMA. Протоколи із

ініціатором отримувачем, які вирішують проблему ПНВ це: RI-BTMA, MACA-BI, а ПВ MARCH.

Протоколи із механізмом резервації поділяються на синхронні та асинхронні. В даних протоколах для здійснення передавання відбувається резервування пропускної здатності, також підтримується QoS. В протоколах, які входять до категорії синхронних вирішуються проблеми ПНВ: NCAC-MAC, D-PRMA, CATA, FPRP, SRMA/PA, HRMA, а в асинхронних, лише проблема ПВ: MACA/PR, RTMAC.

У протоколах із механізмом планування для доступу до середовища, перед передаванням відбувається планування пакетів для забезпечення пріоритетів серед потоків. Протоколи даної категорії орієнтовані на вирішення проблеми ПВ: DPS, DWOP, DLPS.

Протоколи, такі як: H-NAME, MPR-Tree, DPCF, Graph and Beacon використовують управління шляхом маршрутизації, та дозволяють вирішувати проблему ПВ.

Остання категорія описує протоколи із управлінням потужністю та спрямованістю антени. Серед протоколів із управлінням потужністю вирішує проблему ПНВ: PCM, а проблему ПВ: RBAR, ERBAR. Управління спрямованістю дає можливість вирішувати проблему ПНВ, до цієї категорії належать протоколи DBTMA/DA, MACA-D.

Висновки. На основі розгляду 32 протоколів MAC рівня, з урахуванням особливостей існуючих варіантів класифікації та останніх версій протоколів, запропоновано класифікацію, в основу якої покладено спосіб доступу до каналу із можливістю вирішення проблеми прихованих та незахищених вузлів.

Література

1. R. Jurdak, C. V. Lopes. A survey, classification and comparative analysis of medium access control protocols for ad hoc networks// IEEE Communications, 2004, volume 6, no. 1.
2. O. Bazan, M. Jaseemuddin. A Survey On MAC Protocols for Wireless Adhoc Networks with Beamforming Antennas // IEEE COMMUNICATIONS SURVEYS, 10 January 2011.
3. L. Boroumand, R. H. Khokhar, L. A. Bakhtiar. A Review of Techniques to Resolve the Hidden Node Problem in Wireless Networks// Smart Computing Review, vol. 2, no. 2, April 2012.
4. MAC Protocols for Ad Hoc and Sensor Networks// Computer and Communication Systems, [WSN] Winter 2011/2012.
5. D. A. Moltchanov. MAC protocols// TUT, 2011.
6. C. Prakash. Ad Hoc Wireless Media Access Protocols// Lovely Professional University, Punjab 2013
7. J. P. Sheu. MAC Protocols for Ad Hoc Wireless Networks// 2014
8. А.П. Войтер. Media Access Control-уровень сверхширокополосных импульсных радиосетей// УСиМ, 2014, № 3.

УДК 621.396.662.072.078

АНАЛІЗ ФУНКЦІОНУВАННЯ СКЛАДНОГО ОБ'ЄКТУ СИСТЕМИ УПРАВЛІННЯ В ТЕЛЕКОМУНІКАЦІЯХ

Дищук А.С.
Державний університет телекомунікацій, Україна
E-mail: adishuk@mail.ru

Analysis of complex object functioning in control system in telecommunications

The problems of algorithmic analysis and synthesis of control systems of telecommunications networks in future generations are investigated. The basic requirements and problems of modern telecommunications control systems are determined as complex technical systems. The basic characteristic features of complex control object: the need for mathematical description, stochasticity behavior, capacity for evolution, transience complex control object, non-reproducibility of experiments.

Для досягнення високого рівня доступності до інформаційних ресурсів, реалізації вимог ринку інфокомунікаційних послуг потрібна така розвинена система, яка забезпечила б ефективне використання телекомунікаційних комплексів і нових інформаційних технологій. Перехід до мереж майбутніх поколінь (FN) можна вважати радикальною модернізацією телекомунікаційної системи.

Алгоритмічний аналіз управління є основою для прийняття рішення про створення системи управління. При цьому аналізі слід враховувати фактор складності об'єкта управління. Справа в тому, що управління простим об'єктом не представляє труднощів. Всі труднощі управління визначаються складністю об'єкта, тому варто починати саме з об'єкта, а не з алгоритму управління ним. Проаналізуємо зміст *«складного об'єкту управління»*, який досить точно відповідає тому поняттю, яке використовується в теорії управління [1, 2].

Розглянемо основні (але не формальні) ознаки складного об'єкта управління [3,4]:

1. Відсутність математичного опису і необхідність у ньому є обов'язковою ознакою складного об'єкта управління. Під математичним описом маємо на увазі наявність алгоритму (правил, інструкції) обчислення стану *Y* об'єкта за спостереженнями входів - керованого *U* і некерованого, але спостережуваного *X*.

Математично задача зводиться до відшукання якнайкращих показників управління.

При проектуванні системи управління необхідно врахувати, що апріорні імовірності $P(Y_i)$ виникнення тієї або іншої непередбаченої ситуації в мережі наперед не можуть бути визначені і умови виникнення аварійних

ситуацій можуть визначатися за максимальним значенням умовного ризику:

$$R_{\max} = \max_i \sum_{i=1}^{k} P(\hat{y}_i \mid y_i) L_i ,$$

де L_i – деякий нормований коефіцієнт, що характеризує величину втрат в тій або іншій ситуації. Проте знаходження «якнайгіршого» розподілу представляє, як правило, вельми складну самостійну задачу, так що практично зводиться деколи до чисто евристичного вибору «якнайгіршого» розподілу. Так, наприклад, за відсутності яких-небудь апріорних відомостей як «найгірше» часто вибирають нормальний розподіл.

2. Стохастичність поведінки складних об'єктів управління є також дуже важливою ознакою, що характеризує труднощі процесів аналізу та управління ними. Ця ознака зумовлена не стільки наявністю якихось спеціальних джерел випадкових перешкод в об'єкті управління, скільки складністю об'єкта і пов'язаним з цим неминучою великою кількістю різного роду другорядних (з погляду цілей управління) процесів – випадкових чинників. Це ускладнює прогнозування поведінки об’єкта управління, особливо тоді, коли є великий спектр зовнішніх впливів.

3. Здатність до еволюціонування в часі. Структура таких систем і їх функціонування не залишаються незмінними в часі. Проілюструвати твердження можна на прикладі телекомунікаційної мережі, яка є об’єктом управління. Нині телекомунікаційна мережа, яка виникла шляхом еволюції від розрізнених локальних мереж через об’єднання мереж в єдину світову Глобальну інформаційну інфраструктуру, використовується не тільки за своїм прямим призначенням, але і є мережею передавання даних між ЕОМ.

Складність прогнозування можливої еволюції структури для об’єкта типу різнорідної телекомунікаційної мережі унеможливлює застосування централізованої системи управління, яка забезпечила б роботу мережі. Лише перехід до децентралізованого управління, управління локальними підсистемами з локальними функціями забезпечив би доцільне використання можливостей різнорідної телекомунікаційної мережі.

4. «Нетерпимість» до управління є, мабуть, самою прикрою ознакою складного об'єкта управління, утруднює управління ним. Справа в тому, що складний об'єкт існує і функціонує незалежно від суб'єкта і його потреб. Управління має зовнішній характер по відношенню до об'єкта. Природно, що будь-яке управління порушує «нормальне» функціонування об'єкта, тобто змінює його самостійну поведінку і робить залежним від суб'єкта.

5. Нестаціонарність складного об'єкта управління природно випливає з його складності. Ця риса проявляється в дрейфі характеристик об'єкта, в «упливанні» його параметрів, тобто в еволюції об'єкта з часом. Чим складніший об'єкт, тим рельєфніше проявляється ця його риса, що створює серйозні труднощі при синтезі моделі такого складного об'єкта і управлінні ним. Чим складніший об'єкт, тим швидше він змінюється.

Наслідком нестаціонарності є наступна суттєва ознака складного об'єкта.

6. Невідтворюваність експериментів. Проявляється ця ознака в різній

реакції об'єкта на одну й ту ж ситуацію або управління в різні моменти часу. Складний об'єкт весь час ніби перестає бути самим собою, тобто *E* постійно змінюється. Це потрібно враховувати при синтезі моделі об'єкта управління, для чого вводиться її корекція. Всі ці обставини призводять до того, що мета управління таким об'єктом повною мірою ніколи не досягається. Дійсно, для синтезу управління *U* потрібен час, за якого об'єкт змінюється непередбаченим чином, в результаті це управління вже напевно не приведе до бажаного результату *Z**.

Ефективним способом боротьби з перерахованими властивостями складного об'єкта управління є екстраполяція поведінки системи, тобто з'ясування напряму її еволюції. У цьому випадку управління *U* проводиться з попередженням, з урахуванням зміни об'єкта. Інший спосіб полягає в скороченні циклу управління, щоб за час синтезу управління об'єкт сильно не змінився.

Висновок. В результаті проведеного аналізу складного об'єкту управління визначено, що вибір і обґрунтування мети (об'єкту) передбачають визначення показників якості (критеріїв ефективності роботи системи управління) і цільових функцій, які якнайповніші відображають цілі. Отже, складний об'єкт управління відрізняється від системи взагалі тим, що він створений елементами, пов'язаними відношенням, що володіють властивістю здатності об'єкта перебувати у станах із заданої цільової множини. Зазначена необхідність станам складного об'єкта відповідати цільовій множині системи і утворює залежність об'єкта від цілей управління. Встановлено, що всі труднощі управління визначаються складністю об'єкта, тому аналіз необхідно починати саме з об'єкта, а не з алгоритму управління ним. Сформульовано основні характерні ознаки складного об'єкта управління:*необхідність* математичного опису є обов'язковим; *стохастичність* поведінки; *здатність* до еволюціонування; «*нетерпимість*» до управління; *нестаціонарність* складного об'єкта управління природно випливає з його складності; *невідтворюваність* експериментів.

Література

1. Бертсекас Д. Сети передачи данных / Д. Бертсекас, Р. Галлагер. – Москва: Мир, 1989.– 544 с.
2. Гаранин М. В. Системы и сети передачи информации / М.В.Гаранин, В.И. Журавлев, С.В.Кунегин. – Москва: Радио и связь, 2001. – 320с.
3. Математичні основи теорії телекомунікаційних систем / В.В. Поповський, С. О. Сабурова, В. Ф. Олійник, Ю. І. Лосєв, Д. В. Агеев, Т. Г. Калєкіна, О. В. Лемешко, О. Ю. Євсеєва, Ю. Ю. Коляденко, І. В. Стрелковська, Л. О. Титаренко, Д.А. Зайцев. – Харків : СМІТ, 2006. – 564 с.
4. Окунев Ю. Б. Принципы системного перехода к проектированию в технике связи / Ю. Б.Окунев, В. Г.Плотников. – Москва: Связь, 1976.–184с.

УДК 621.396.4

ИССЛЕДОВАНИЕ МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ НА ОСНОВЕ СТАНДАРТА 802.11N

Осипчук И.С., Чекунов Н.В., Осипчук С.А.
Институт телекоммуникационных систем, НТУУ «КПИ», Украина
E-mail: osypchuk_ivan@i.ua

Research of the multiservice communication network based on the 802.11n standard

We used the modern wireless communication standard IEEE 802.11n to develop a multiservice point-to-point network based on 802.11n equipment. We tested different types of traffic and its combinations transmitted via high data rate wireless channel: audio stream, video stream and data transfer. We compared the measured data rates values with recommended by standard, and shown the correlation between them. We show by the same the applicability of 802.11n wireless SDR transceivers for building the multiservice networks.

Большинство сетей связи для конечного пользователя на сегодняшний день являются мультисервисными сетями, проводными или беспроводными. Такие инфокоммуникационные сети связи разработаны и адаптированы для предоставления множества информационно-телекоммуникацинных услуг: передачи голоса, данных, видео, и др. Основная задача мультисервисных сетей заключается в предоставлении конечному абоненту набора услуг, при этом транспортная компонента для них унифицирована, требует наличия совместной среды для передачи сигналов, наличия единых протоколов и соответствующего приемопередающего оборудования. Такое оборудование, как правило, соответствует концепции SDR (software defined radio).

Стандарт IEEE 802.11n [1,2] представляет собой один из передовых стандартов беспроводной связи LAN сетей, описывающий физический и канальный уровень согласно модели OSI. На основе стандарта 802.11n можно строить мультисервисные сети с использованием, например, стека TCP/IP на сетевом и транспортном уровнях модели OSI. Оборудование 802.11n предоставляет доступное подключение для сетей передачи данных, покрывая требуемую зону охвата, ширину канала и производительность, необходимые для современных мультимедиа-приложений и сервисов. Оборудование 802.11n также может использоваться для построения беспроводных сегментов MAN сети для передачи мультисервисного трафика [3] в случае применения направленных антенн.

В данной работе проведено исследование мультисервисной сети для передачи разных видов трафика на основе оборудования 802.11n по схеме точка-точка (рис. 1). Схема для испытаний реализована с помощью двух конечных терминалов (ПК), которые подключены к точкам доступа 802.11n Mikrotik SXT Lite5.

В исследуемой сети рис. 1 использованы следующие устройства:

1) MikroTik RouterBOARD SXT lite5 [2 шт.] – приемопередатчик стандарта 802.11a/n MIMO диапазона 5 ГГц с направленной антенной.

Встроенная антенна 16dBi MIMO 2x2 позволяет устанавливать связь с канальной скоростью до 300 Мбит/с на небольшие расстояния.

2) Конечный терминал пользователя, TCP/IP совместимый [2 шт.] – использованы ПК с интерфейсом Ethernet.

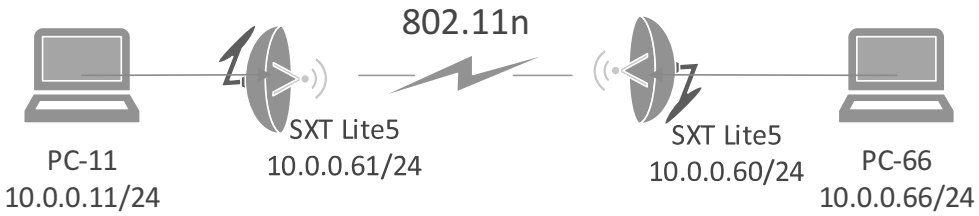


Рис. 1. Исследуемая сеть вида точка-точка на основе оборудования 802.11n

Максимально достигнутая скорость передачи TCP трафика в исследуемой сети при определенных энергетических условиях равна 80 Мбит/с. В сети производилась одновременная передача разного сетевого трафика, а именно: трансляция видеопотока в стандарте MPEG-2, трансляция аудиопотока, передача файла данных.

Любая мультисервисная сеть должна поддерживать ключевые виды сервисов. В табл. 1 содержится список некоторых из наиболее распространенных Wi-Fi Multimedia (WMM) категорий сервисов. Каждый вид услуги включается в одну из четырех категорий, получающих привилегированный доступ к среде (QoS). В порядке убывания приоритета, трафик может быть помещен в очереди для передачи голоса, видео, очередь с наилучшим усилием, и фоновый трафик.

Таблица 1. Виды услуг мультисервисной сети, рекомендации по необходимой скорости и группы WMM

Вид сервиса	***Рекомендуемая скорость передачи данных (Мбит/с)***	***Категория сервиса***
VoIP-трафик	27 – 93 кбит/с	Голос
VoIP-сигнальный трафик	5 кбит/с	Наилучшее усилие
Удаленный рабочий стол	150 кбит/с – 1.8 Мбит/с	Голос
Веб конференция	384 кбит/с – 1 Мбит/с	Голос
ТВ видео поток	2.5 – 8 Мбит/с	Видео
Видео высокой четкости (сжатое)	2 – 5 Мбит/с	Видео
Видео высокой четкости (несжатое)	20 Мбит/с	Видео
Видео высокой четкости (несжатое HDTV)	3.3 Гбит/с	Видео
Видео обычной четкости	1 – 1.5 Мбит/с	Видео
Емейл/просмотр Веб-страниц	0.5 – 1.0 Мбит/с	Наилучшее усилие
Обмен файлами	5 Мбит/с	Наилучшее усилие
YouTube	0.9 Мбит/с	Наилучшее усилие

Качество предоставления услуг (QoS) включает в себя соблюдение требований к Wi-Fi Multimedia (WMM) сертификации, которая разделяет

категории сервисов на четыре класса с различным приоритетом. Другие подходы к организации очередей могут быть использованы для повышения качества обслуживания определенных сервисов, в зависимости от постановки задачи.

Экспериментальная часть исследования сети рис. 1 включала трансляцию аудиопотока (MP3), видеопотока (MPEG-2), что выполнено с помощью программного продукта Ace Stream Media Center. Для передачи данных проводился тест скорости передачи файла данных между FTP сервером и клиентом. В табл. 2 предоставлены данные о состоянии интерфейсов подключения и скоростях передачи, измеренных в утилите Winbox.

Таблица 2. Результаты измерения скорости передачи данных в случае

Вид сервиса	***Измеренная скорость передачи данных (Мбит/с)***
Аудио-поток MP3	0.145
Видео-поток MPEG-2	5.9
Два видео-потока MPEG-2	12.2
Передача файла данных	69.6
Одновременно аудио-поток, видео-поток и передача файла данных	72.4

Скорость передачи файла данных при одновременном потоке аудио, видео и передачи файла уменьшилась с 69.6 Мбит/с до 65.5 Мбит/с, что связано с динамическим распределением ресурса канала и учетом QoS для разных видов трафика, как и ожидается в случае мультисервисной сети.

Таким образом, экспериментально показано, что на основе стандарта IEEE 802.11n можно организовывать мультисервисные беспроводные сети связи: осуществлять одновременную передачу потокового аудио, видео, передачу файлов, с обеспечением требуемых предопределенных QoS.

Литература

1. L. Usryvsky, S. Osypchuk, B. Shmigel. The 802.11 Protocols Usage for Wireless Systems Construction with Flexible Architecture. TCSET'2016, February 23–26, 2016, Lviv-Slavske, Ukraine. pp. 918-921.
2. IEEE Standard 802.11n-2009 – IEEE Standard for Information technology – Local and metropolitan area networks – Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput. Электронная версия доступна по ссылке: https://standards.ieee.org/findstds/standard/802.11n-2009.html.
3. Гургенидзе А.Т., Кореш В.И. Мультисервисные сети и услуги широкополосного доступа. СПб, Наука и техника, 2003. – 400 с.

УДК 621.391

КЛАСИФІКАЦІЯ МОДЕЛЕЙ ПЕРЕМІЩЕННЯ ВУЗЛІВ У МЕРЕЖАХ MANET

Максимов В.В., Кулик М.В.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: maksimov46@ukr.net, maryna.kulyk2015@gmail.com

Classification of node mobility models in MANET networks

An overview of mobility models and their most important features are provided.

Для систем, пов'язаних з мобільними вузлами, переміщення рухомих вузлів має значний вплив на результати моделювання. Тому модель мобільності є одним з найважливіших компонентів при моделюванні мереж MANET.

Метою даної роботи є побудова класифікації моделей мобільності в залежності від їх конкретних характеристик мобільності. В основі пропонованої класифікації лежать існуючі класифікації моделей переміщення [1, 4, 5, 6, 7, 8], які пропонується розширити та доповнити.

Класифікація проведена за наступними характеристиками: за залежністю між вузлами; за рівнем розподілу, або деталізації; за рівнем випадковості; за технікою утворення; за класом мобільної сутності (користувача); моделі з обмеженнями.

1.1. Поділ моделей за ознакою залежності між вузлами. Моделі переміщення можна розділити на 2 великі групи: індивідуальні та групові моделі переміщення [2, 8]. В індивідуальних (незалежних) моделях мобільні вузли переміщуються незалежно один від одного в межах області моделювання. В групових моделях всі вузли переміщаються разом колективно.

До індивідуальних моделей належать: *модель на основі випадкових маршрутних точок* [1, 2]; *модель на основі випадкового (броунівського) руху* [2]; *модель на основі випадкового напрямку* [2]; *модель гауса-маркова* [1, 2]; *семі-марківська модель мобільності* [1]; *модель з необмеженою областю моделювання* [2].

До групових моделей належать: *колонна модель* [2]; *модель з переслідуванням* [2]; *модель потоку рідини* [2]; *кочова модель* [2]; *общинна модель мобільності* [1]; *модель переміщення з груповою опорною точкою (rpgm)* [1, 2]; *модель оптимальної швидкості ньюела* [8]; *модель слідування за лідером дженерал моторс* [8]; *модель «розумного водія» трайбера* [8].

1.2. Поділ моделей за рівнем розподілу, або деталізації. Переміщення вузлів у мережі можна порівняти з переміщенням автомобілів на дорогах, трасах тощо. В зв’язку з цим і виникли моделі переміщення вузлів, аналогічні моделям транспортних потоків, які за рівнем розподілу (рівнем деталізації) можна виокремити в *мікроскопічні*, *мезоскопічні* та *макроскопічні*[3, 8].

1.3. Поділ моделей за рівнем випадковості. За рівнем випадковості моделі діляться на випадкові, постійні та гібридні [4, 6, 7, 9].

До випадкових моделей належать: *модель на основі випадкових маршрутних точок; модель на основі випадкового напрямку; модель на основі випадкового (броунівського) руху; експоненціально корельована модель випадкових переміщень* [8]. в*ипадкова ймовірнісна модель* [9].

До постійних моделей належать: *модель на основі постійної позиції*; *модель на основі постійної швидкості*; *модель на основі постійного прискорення*.

До гібридних (змішаних): *модель зі зваженою точкою* [6]; *модель переміщення в міських кварталах* [6].

1.4. Поділ моделей за технікою утворення. Моделі переміщення можна поділити на простежувальні та комплексні [1].

Простежувальні моделі будуються на основі мап. До них відносяться: *проста людська модель* [6]; *модель мобільності «автострада»* [6, 7]; *манхетенська модель* [6,7]; *модель мобільності «година пік»* [6].

До комплексних моделей відносяться: *модель гауса-маркова; модель на основі випадкових маршрутних точок; модель на основі випадкового напрямку; модель на основі випадкового руху; випадкова ймовірнісна модель*.

1.5. Поділ моделей за класом мобільної сутності (користувача) [10].

Засіб пересування користувача мережі впливає на можливі місця розташування і швидкість руху цього користувача. Транспортні засоби не можуть виходити на пішохідні вулиці і пішоходи не можуть переходити на автомагістралі. Таким чином всі простежувальні моделі можна розділити на транспортні засоби та пішоходів (людей).

1.6. Моделі з обмеженнями [7] поділяються на моделі з географічними обмеженнями, моделі з просторовою залежністю і моделі з часовою залежністю.

Моделі з географічними обмеженнями: *модель з урахуванням шляху; модель з урахуванням перешкод; модель на основі мап*.

Моделі з просторовою залежністю: *модель групових переміщень з опорною точкою (RPGM) та ін*..

Моделі з часовою залежністю: *модель гауса-маркова; гладка випадкова модель мобільності*.

На основі проведеного аналізу моделей переміщення вузлів у мережах MANET побудована класифікація, яка представлена на рис. 1. Розглянуті моделі переміщення поводяться по-різному і впливають на продуктивність протоколу і результати моделювання. Тому, вкрай важливо використовувати багатий набір моделей мобільності. Дана класифікація може бути корисна при

моделюванні мереж MANET.

Рис. 1 Класифікація моделей переміщення вузлів у мережах MANET.

Література

1. Elmano Ramalho Cavalcanti, Marco Aurélio Spohn (2013). *On the Interactions between Mobility Models and Metrics in Mobile ad hoc Networks*. International Journal of Networks and Communications.
2. Anuj K Gupta, Harsh Sadawarti, Anil Kumar Verma (2013). *Performance Analysis of MANET Routing Protocols in Different Mobility Models*. Article in Journal of Computing and Information Technology.
3. Mihails Savrasovs. *Исследование возможности использования мезоскопического подхода для моделирования транспортных потоков*. M.SC.COMP.
4. Mihail L. Sichitiu. *Mobility Models for Ad Hoc Networks*. NC State University: Dept. of Electrical and Computer Eng., Campus Box 7911.
5. Amit Kumar Chaturvedi, Jitendra Kumar (2014). *Analysis of Mobility Models in Mobile Ad-hoc Networks* . Poornima University: International Journal of Computer Applications (0975 – 8887) National Seminar on Recent Advances in Wireless Networks and Communications.
6. *A Survey on Mobility Models for Wireless Networks* (2011): SITI Technical Report SITI-TR-11-01.
7. Fan Bai, Ahmed Helmy. *A SURVEY OF MOBILITY MODELS in Wireless Adhoc Networks*. U.S.A: University of Southern California.
8. И.О. Датьев. Модели перемещения сетевых узлов для исследования протоколов маршрутизации мобильных самоорганизующихся сетей.УДК 004.7, 004.4: Институт информатики и математического моделирования технологических процессов Кольского НЦ РАН Кольский филиал Петрозаводского государственного университета.
9. Ejiro .E. Igbesoko, Thaddeus Onyinye Eze, Mona Ghassemian (2010).*Performance Analysis of MANET Routing Protocols over Different Mobility Models*. London: School of Computing and Mathematical Sciences University of Greenwich.
10. S. Nousiainen, K. Kordybach, P. Kemppi, User distribution and mobility model framework for cellular network simulations, in: VTT Information Technology, 2002, pp. 518–522.

УДК 621.3

ТУННЕЛИРОВАНИЕ И ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ НА ОСНОВЕ MPLS

Гаттуров В.К., Цыпанов В.А.
Институт телекоммуникационных систем
E-mail: v.tsipanov@hotmail.com

Tunneling and VPNs based on MPLS

This article deals with the architectural VPN solutions in packet-switched networks. It is demonstrated that almost all solutions except MPLS-VPN are insufficient for traffic multiplexing, good QoS and data encapsulation. Also in article compares the tunneling principle for these solutions.

Наиболее универсальным способом построения VPN является использование технологии инкапсуляции, или туннелирования. В общем случае туннелирование применяется для того, чтобы передавать пакеты одной сети (первичной) по каналам связи другой (вторичной), протоколы которых не совместимы. Для этого пакеты первичной сети (данные и протоколы) инкапсулируется в пакеты вторичной сети, и становятся видны как данные. Таким образом, пакет продвигается маршрутизаторами ядра сети только на основании внешнего заголовка, без инспекции содержимого оригинального пакета. Далее приводится краткое описание наиболее распространенных решения по туннелированию при создании виртуальных частных сетей.

Протокол PPTP. Протокол PPTP (Point-to-Point Tunneling Protocol) позволяет инкапсулировать (упаковывать или скрыть от использования) пакеты PPP в пакеты протокола Internet Protocol (IP) и передавать их по сетям IP (в том числе и Интернет).

Протокол PPTP обеспечивает безопасную передачу данных от удаленного клиента к отдельному серверу предприятия путем создания в сети TCP/IP частной виртуальной сети. Протокол PPTP может также использоваться для организации туннеля между двумя локальными сетями.

Протокол L2TP. Протокол L2TP (Layer 2 Tunneling Protocol) - протокол туннелирования канального уровня, который позволяет организовывать VPN с заданными приоритетами доступа, однако не содержит в себе средств для защиты данных и механизмов аутентификации.

Протокол L2TP использует сообщения двух типов: управляющие и информационные сообщения. Управляющие сообщения используются для установления, поддержания и ликвидации туннелей и вызовов. Для обеспечения доставки ими используется надежный управляющий канал протокола L2TP. Информационные сообщения используются для инкапсуляции кадров PPP, передаваемых по туннелю. При потере пакета он не передается повторно.

Протокол IPSec. Другой очень популярный протокол для построения VPN - IPSec в режиме туннелирования. Напомним, что туннельный режим устанавливается для шлюзов и является, по существу, IP-туннелем с аутентификацией и шифрованием. Им предусматриваются два набора IP-заголовков: внешний и внутренний. Первый содержит IP-адрес VPN-шлюза, тогда как второй - IP-адрес конечной системы.

Протокол IPSec может быть полезен для любой VPN даже без его

туннельных свойств: какой бы тип VPN ни применялся, если нужно спрятать информацию от чужих глаз, то можно воспользоваться транспортным режимом IPSec поверх основного транспорта.

MPLS VPN. Технология MPLS позволяет пересылать данные с помощью меток, прикрепляемых к каждому пакету. Внутренние узлы ядра сети, поддерживающие MPLS, не нуждаются в анализе содержимого каждого пакета. Так, не рассматривается IP-адрес получателя, что дает возможность MPLS предоставить эффективный механизм инкапсуляции для частного трафика, передаваемого по магистрали оператора. Имея это в виду, сформированные протоколом распределения меток (Label Distribution Protocol, LDP) маршруты продвижения пакетов от отправителей к получателям (Label Switched Path, LSP) нередко рассматривают как туннели через всю сеть MPLS или через ее магистральную часть.

Основой любого решения является использование LSP-туннеля для продвижения данных между фронтальными маршрутизаторами поставщика услуг, которыми ограничивается определенная VPN. Присваивая метки соответствующим пакетам, LER и LSR надежно отделяют VPN-потоки от остальных данных, передающихся по магистрали. Это разделение представляет собой ключевой механизм, посредством которого MPLS может поддерживать следующие характеристики VPN-туннелирования:

- инкапсуляция данных независимо от применяемых протоколов, поскольку пакеты передаваемые по туннелю непрозрачны для промежуточных маршрутизаторов, формирующих магистраль;
- мультиплексирование трафика различных VPN, передаваемого по разделяемой магистрали, посредством использования отдельных LSP-туннелей для каждого источника данных;
- аутентификацию конечных точек LSP-туннелей с помощью протоколов распределения меток (LDP);
- обеспечение необходимого уровня QoS путем резервирования сетевых ресурсов для LSP-туннеля. MPLS поддерживает как IntServ, так и DiffServ;
- надежную коммутацию и автоматическое перенаправление LSP-туннеля за счет исключения неисправного канала или маршрутизатора без вмешательства администратора.

Сравнительный анализ туннелей MPLS и обычных туннелей. Туннели MPLS позволяют передавать данные любого протокола вышестоящего уровня (например IP, IPX, кадры Frame Relay, ячейки ATM), так как содержимое пакетов вдоль всего пути следования пакета остается неизменным, меняются только метки. В отличие от них, туннели IPSec поддерживают передачу данных только протокола IP, а протоколы PPTP и L2TP позволяют обмениваться данными по протоколам IP, IPX или Net BEUI. Безопасность передачи данных в MPLS обеспечивается за счёт определённой сетевой политики, запрещающей принимать пакеты, снабжённые метками, и маршрутную информацию VPN-IP от непроверенных источников. Она может быть повышена использованием стандартных средств аутентификации и/или шифрования (например шифрование IPSec). Для безопасной передачи данных в протокол IP Security включены определенные процедуры шифрования IP-пакетов, аутентификации, обеспечения защиты и целостности данных при транспортировке, вследствие чего туннели IPSec обеспечивают надежную доставку информационного трафика.

Протокол L2TP поддерживает процедуры аутентификации и туннелирования

информационного потока, а PPTP помимо данных функций снабжен и функциями шифрования. Применение меток MPLS позволяет реализовать ускоренное продвижение пакетов по сети провайдера. Транспорт MPLS не считывает заголовки транспортируемых пакетов, поэтому используемая в этих пакетах адресация может носить частный характер. Содержимое пакетов не считывается и при передаче IP-пакетов по протоколам IPSec, PPTP и L2TP. Однако, в отличие от MPLS, традиционные протоколы туннелирования для транспортировки IP-пакетов используют традиционную IP-маршрутизацию. При выборе пути следования пакета в MPLS учитываются различные параметры, оказывающие влияние на выбор маршрута. Совместная работа технологии многопротокольной коммутации и механизмов Traffic Engineering позволяет для каждого туннеля LSP предоставить требуемый уровень качества обслуживания за счет процедуры резервирования ресурсов на каждом маршрутизаторе вдоль пути следования пакета. Помимо этого, появляется возможность отслеживать действительный маршрут, проходящий через сформированный туннель, возможность диагностики и административного контроля туннелей LSP. Различные туннели, в соответствии с необходимым уровнем QoS между двумя точками поддерживает и протокол L2TP.

Технология VPN IPSec не поддерживает параметров качества обслуживания установленного соединения, а протокол PPTP поддерживает единственный туннель между двумя точками. Нельзя не отметить и тот факт, что весь трафик при использовании традиционных IP-туннелей следует до адресата вдоль одного и того и того же пути. Технология MPLS позволяет контролировать потоки, передаваемые по множеству всех имеющихся путей до адресата.

В качестве вывода покажем, какие возможности предоставляют туннели в MPLS:

1. Возможность формирования LSP-туннелей с или без требований QoS.
2. Возможность динамически изменять маршруты сформированных LSP туннелей.
3. Возможность отслеживать действительный маршрут, проходящий через сформированный LSP туннель.
4. Возможность идентифицировать и диагностировать LSP туннели.
5. Возможность устанавливать сформированный LSP туннель под административный контроль.
6. Возможность осуществлять посылку запросов выделения меток, их рассылку и объединение.

И как следствие MPLS-VPN предлагает улучшенную производительность по сравнению с IP-VPN, потому что, у вас есть возможность разделить ваши данные на различные категории, такие как реальное время трафика, приоритет трафика, низкий приоритет трафика и так далее. Ваш оператор мобильной связи будет поддерживать эти приоритеты по всей своей сети, обеспечивая качество обслуживания в любом конце. Также MPLS поддерживает высокий уровень безопасности, так как трафик сегментирован от других пользователей на сети оператора.

Литература

1. Семенов Ю.А. «Телекоммуникационные технологии». – «Москва», 2014. – 600с.
2. А.Б. Гольдштейн, Б.С. Гольдштейн «Технология и протоколы MPLS». – «БХВ – Санкт-Петербург», 2005. – 306с.
3. Вивек Олвейн «Структура и реализация современной технологии MPLS», «Москва», 2010 г. – 606с.

УДК 621.39

ЗАХИСТ ТРАНСПОРТНИХ МЕРЕЖ ВІД DDoS АТАК

Гаттуров В.К., Шаповалов Р.С.
НТУУ «КПІ» Інститут телекомунікаційних систем
E-mail: sharom94@gmail.com

Protection transport network from DDoS attacks

The article describes the main types of DDoS-attacks and how they affect the transport network provider of telecommunications services. The article also describes some of the main methods to combat DDoS-attacks, and explained what effect do these methods to suppress the attacks.

Розподілені мережеві атаки часто називають атаками типу «відмова в обслуговуванні» (Distributed Denial of Service, DDoS). Успіх атак цього типу зумовлений обмеженням пропускної здатності, яка є однією з характеристик будь-якого мережевого ресурсу, наприклад інфраструктури. Під час DDoS-атаки ресурсу надсилається велика кількість запитів із метою вичерпати його можливості обробки даних і порушити нормальне функціонування.

Мережеві ресурси (наприклад, веб-сервери) завжди мають обмеження щодо кількості одночасно оброблюваних запитів. Крім обмеження потужності сервера, канал, яким сервер зв'язується з Інтернетом, також має скінченну пропускну здатність. Якщо число запитів перевищує граничні можливості якого-небудь компонента інфраструктури, можуть виникнути такі проблеми з рівнем обслуговування:

- формування відповіді на запити відбувається значно повільніше, ніж зазвичай,
- деякі або навіть всі запити користувачів можуть залишитися без відповіді.

Зазвичай кінцева мета зловмисника – цілковите припинення нормальної роботи веб-ресурсу, цілковита «відмова в обслуговуванні».

Атаки можна класифікувати за наступними ознаками:

а) За характером впливу (пасивний вплив, активний вплив),

б) По меті впливу (порушення конфіденційності інформації або ресурсів системи, порушення цілісності інформації, порушення працездатності (доступності) системи),

в) За умовою початку здійснення впливу (атака на запит від об'єкта що атакується, атака по настанню очікуваної події на об'єкті що атакується, безумовна атака),

г) За наявності зворотнього зв'язку з атакуючим об'єктом (зворотнім зв'язком, без зворотнього зв'язку (односпрямована атака)),

д) По розташуванню суб'єкта атаки щодо об'єкта який атакується

(внутрішньо сегментний, міжсегментний),

е) За рівнем еталонної моделі ISO / OSI, на якому здійснюється вплив (фізичний, канальний, мережевий, транспортний, сеансів, представницький, прикладної).

Атаки в транспортних мережах.

В транспортних мережах DDoS атаки розглядаються на двох рівнях моделі OSI, а саме це L2 (Канальний) та L3 (Мережевий).

На L2 DDoS атаки це — «забивання» каналу. Це атаки, які спрямовані на позбавлення доступу до зовнішньої мережі внаслідок вичерпання канальної ємності. Абсолютно неважливо, яким саме чином. Як правило, для цієї мети використовуються масовані, з точки зору трафіку, атаки типу «що-небудь»-Amplification (NTP-, DNS, RIP-… Amplification може бути будь-який, не має сенсу перераховувати). Взагалі, до цього класу атак відносяться всілякі flood-и, в тому числі ICMP Flood і т.д. Основне завдання полягає в тому, щоб в канал розміром, скажімо, 1 Гігабіт/с залити хоча б 1,1 Гігабіт/с. Цього буде достатньо для припинення доступу.

На L3 DDoS атаки це — порушення функціонування мережевої інфраструктури. До цього класу відносяться, серед іншого, атаки, що приводять до проблем з маршрутизацією в рамках протоколу BGP, з анонсами мереж (Hijacking) — або атаки, наслідком яких стають проблеми на транзитному мережевому обладнанні: наприклад, переповнення таблиці відстеження сполук. Атаки даного класу відрізняються великою різноманітністю.

Захист від атак.

В залежності від типу атаки та рівня моделі OSI використовуються різні методи захисту від DDoS атаки.

На рівні L2, якщо смуга атаки перевищує 100 Гігабіт/с, то ці гігабіти потрібно десь обробляти, наприклад, на стороні провайдера або датацентру, і проблема завжди буде в «останньої милі». За допомогою технології BGP Flow Spec можна фільтрувати частина атак по сигнатурах пакетів — скажімо, Amplification легко відсікається по порту джерела. Однак подібний спосіб досить дорогий і не від всього здатний захистити.

На рівні L3 необхідно аналізувати мережеву інфраструктуру, причому не тільки свою. Одним з прикладом атак є BGP Hijacking. На жаль, автоматично з подібною напастю боротися неможливо, все доведеться робити вручну. Але до того, як почнеться боротьба, ще потрібно буде визначити, що дана проблема (крадіжка префікса) взагалі виникла. Якщо це сталося, то необхідно звернутися до мережного оператора, до адміністрації датацентру, до хостеру і т. д. Вони допоможуть у вирішенні проблеми. Але для цього потрібна просунута аналітика мережевої інфраструктури, тому що ознакою Hijacking служить, в загальному випадку, тільки те, що, починаючи

з якогось моменту, анонси даної мережі в інтернеті пішли «нетипові», не такі, як були протягом тривалого часу до цього. Відповідно, для своєчасного виявлення необхідно мати, як мінімум, історію анонсів.

Якщо у вас своєї автономної системи (AS) немає, то можна вважати, що боротьба з атаками на цьому рівні більш-менш є обов'язком вашого датацентру (або провайдера). Проте, заздалегідь зазвичай не можна сказати, наскільки той чи інший датацентр серйозно підходить до даної проблеми.

Існує декілька методів боротьби з DDoS атаками:

- На рівні вузла (повинен бути доступ до вузла через інший шлях);
- На рівні мережі (блокується все що може дати більше інформації про вас атакуючому(ping, traceroute));
- На рівні провайдера (аналіз пакетів та блокування підозрілих ip-адрес);
- На рівні обладнання операторів зв’язку (використання обладнання, котре може полегшити боротьбу з атаками внаслідок вбудованих функцій);
- На рівні адміністратора (можливість визначити джерело атаки та спробувати йому завадити);
- Комбінований (використання всіх можливих систем).

Висновки. Проведений аналіз показав, що DDoS атаки поводяться по різному в залежності від рівня моделі OSI та типу атаки. Основними методами захисту та боротьби проти таких атак являється обробка трафіку, який генерується під час атаки, відсікання такого трафіки чи створення певних Firewall на обладнанні.

Можна сказати, що всі перераховані вище методи не покривають і 70% всіх методів боротьби з DDoS атаками і над цією темою, боротьби з DDoS атаками, працює досить багато людей у всьому світі.

Література

1. Атака через INTERNET / Медведовский И.Д., Семьянов П.В., Платонов В.В.;Под ред. проф. Зегжды П.Д. - СПб: Мир и семья-95, 1998. - 296с.
2. Защита **информации** в компьютерных **систем**ах и сетях [Текст] / Романец Ю.В., Тимофеев П.А. / Под ред. Шаньгина В.Ф. - М.: Радио и связь, 2001. - 376 с.
3. http://www.internet-technologies.ru/articles/article_436.html.

УДК 621.396

ОЦІНКА ПАРАМЕТРУ ЕНЕРГОЕФЕКТИВНОСТІ ОПТИЧНИХ ТРАНСПОРТНИХ МЕРЕЖ НА БАЗІ ЕЛЕКТРООПТИЧНИХ ПРИСТРОЇВ

Кайдан М.В., Андрущак В.С.
Національний університет «Львівська політехніка», Україна
E-mail: kaidan_k@mail.ru, volodya1andrushchak@gmail.com

The Estimation Parameter of Energy Efficiency for Optical Transport Network with Using Electro-Optic Devices

In work presented the influence electro-optic coefficient of modulator on energy efficiency of optical transport network. Estimation parameter of energy efficiency was performed on development mathematical and simulation model.

Оптичні модулятори і комутатори визначають енергоспоживання пристроїв DWDM рівня. Як було встановлено в нашій попередній роботі [1] – використання електрооптичного ефекту є кращим для оптичних модуляторів, а акустооптичної взаємодії для оптичних комутаторів.

Волоконнооптичні системи передачі інформації (ВОСПІ) зі швидкістю вище 10Гбіт/с вимагають використання зовнішніх модуляторів [2]. Відповідно об'єктом дослідження стали зовнішні електрооптичні модулятори за запропонованою архітектурою пристрою (див. рис.1).

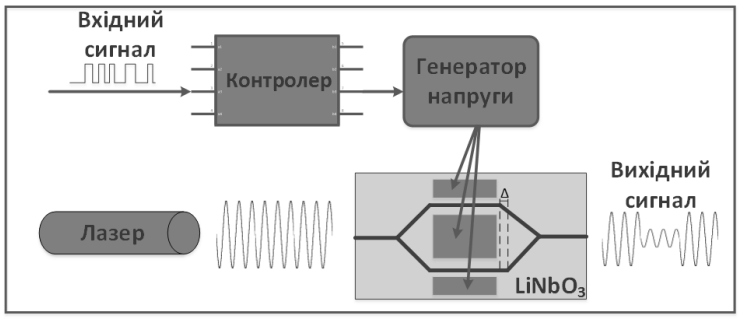


Рис.1 Структурна схема досліджуваного електрооптичного модулятора.

Контролер (процесор) здійснює управління даним модулятором і керуванням роботи генератором напруги. В залежності від значень вхідного сигналу (послідовності 1 і 0) процесор відсилає необхідний сигнал управління генератору напруги. Останній в свою чергу здійснює безпосереднє прикладання керуючої напруги до кристалу ніобату літію.

Виходячи із структури даного електрооптичного модулятора розроблено математичну модель для визначення параметру енергоефективності:

$$P_{\text{mod}}(V) = P_{proc}(v) + P_{genV}(v) + P_{cool}(v), \quad (1)$$

де $P_{proc}(v)$ – енергоспоживання контролера, яке визначається енергоспоживанням процесора, $P_{genV}(v)$ – енергоспоживання генератора напруги, $P_{cool}(v)$ – електроенергія, яка витрачається на охолодження модулятора.

Енергетичне споживання процесора визначається сумою енергоспоживання

наступних елементів: арифметично логічним пристроєм (ALU), тактовим генератором, кешом і елементів пам'яті.

Енергоспоживання кожного з такого елемента визначається наступною формулою [3]:

$$P_{elem} = C \cdot V_{dd}^2 \cdot a \cdot f, \quad (2)$$

де C – агрегаційна ємність навантаження для кожного компонента, V_{dd} – робоча напруга, a – активність кожного елемента для кожного такту генератора ($0 \le a \le 1$), f – тактова частота процесора.

Витрати електроенергії модулятора на його охолодження визначається:

$$P_{cool}(v) = k \cdot (P_{proc}(v) + P_{genV}(v)) \quad (3)$$

Як зазначено в роботі [4] при споживання мережевим пристроєм 1 Вт електроенергії витрачається до 1 Вт електроенергії на його охолодження. Відповідно в розробленій математичній моделі приймаємо параметр k в межах $0,5 \le k \le 1$.

Енергоспоживання генератора $P_{genV}(v)$ визначається півхвильовою напругою, яка необхідна для досягнення електрооптичного ефекту:

$$U_{\lambda/2} = \frac{\lambda \cdot d}{2 \cdot n^3 \cdot r_{ij} \cdot L}, \quad (4)$$

де λ - довжина хвилі, d - товщина зразка, n - показник заломлення, r_{ij} - електрооптичний коефіцієнт, L - довжина кристала.

Відповідно енергетичне споживання генератора напруги визначається за наступною формулою (5):

$$P_{genV}(v) = \int I \cdot U_{manag}(t) dt, \quad (5)$$

де параметр U_{manag} змінюється в діапазоні $0 < U_{manag} < U_{\lambda/2}$.

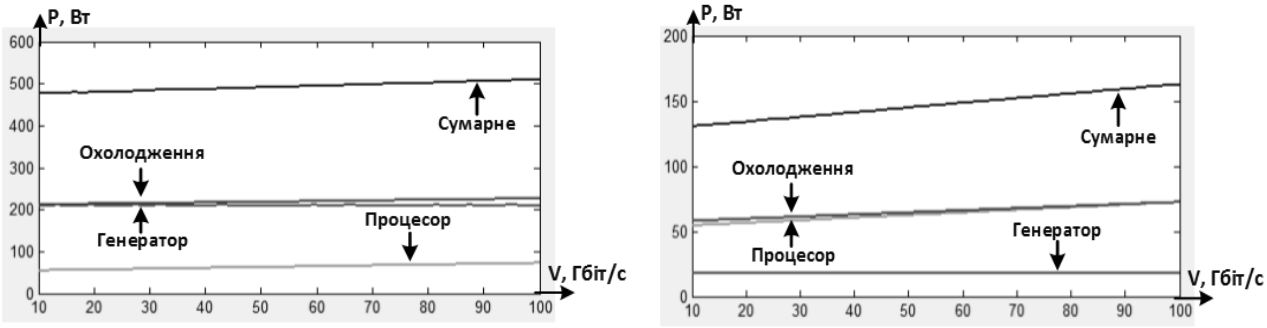
Проведено моделювання для оцінки параметру енергоефективності для електрооптичного модулятора, вхідні дані для якого представлені в таблиці 1.

Таблиця 1. Вхідні дані для моделювання

Параметр	***Значення***	***Параметр***	***Значення***
Процесор		***Параметри кристалу і генератора***	
Напруга, U	1,25 В	Показник заломлення, n	2,2378
Тактова частота, f	2,8ГГц	Довжина хвилі, λ	1555нм
Сукупна ємність навантаження (СЄН) ALU, C_{ALU}	310 пФ	Електрооптичний коефіцієнт, r_{ij}	$3.4*10^{-12}$ м/В $39,7*10^{-12}$м/В
СЄН тактового генератора, C_{clk}	3330 пФ	Товщина зразка, d	13.4мм
СЄН кешу C_C	957пФ	Довжина зразка, L	18,5мм
СЄН кешу і шин C_{mchl}	0,088фФ	Значення струму генератора, I	60мА

Моделювання проведене в діапазоні швидкостей від 10 до 100Гбіт/с для двох значень електрооптичного коефіцієнту – $r_{ij}=3.4*10^{-12}$ м/В [5] і для знайденого значення в роботі [6] – $r_{ij}=39.7*10^{-12}$ м/В.

Як видно із графіків рис. 2 збільшення швидкості передачі призводить до лінійного зростання енергетичного споживання електрооптичного модулятора. Головний чином енергоспоживання процесора (зелена крива) збільшується при підвищені швидкості передачі даних. Це пояснюється тим, що збільшення швидкості призводить до підвищення активності кожного елемента процесора, відповідно $a \to 1$. Слід зазначити, що енергоспоживання генератора напруги практично не змінюється при зміні швидкості передачі.



а) *б)*

Рис. 2 Енергоспоживання електрооптичного модулятора і його компонентів в залежності від швидкості передачі даних при а) rij=3.4*10-12 м/В б) rij=39.7*10-12 м/В.

Таблиця 2. Результати моделювання.

Елемент модулятора	***Енергоспоживання, Вт***	***Елемент модулятора***	***Енергоспоживання, Вт***
r_{ij}=3.4*10^{-12} м/В, швидкість 10Гб/с		**r_{ij}=39,7*10^{-12} м/В, швидкість 10Гб/с**	
Генератор напруги	209,6	Генератор напруги	19,1
Сумарне	475,3	Сумарне	132,5
r_{ij}=3.4*10^{-12} м/В, швидкість 100Гб/с		**r_{ij}=39,7*10^{-12} м/В, швидкість 100Гб/с**	
Генератор напруги	210,5	Генератор напруги	18,9
Сумарне	509,2	Сумарне	164,5

Імітаційна модель дозволила встановити (див табл. 2), що збільшення швидкості передачі даних від 10 до 100Гбіт/с збільшило енергоспоживання процесора на 24,86%. Збільшення загального енергоспоживання відбулось на 33,9Вт (при r_{ij}=3.4*10^{-12} м/В). Для електрооптичної комірки з параметром r_{ij}=39,7*10^{-12} м/В енергоспоживання процесора також збільшилось на 24,86%. Збільшення загального енергоспоживання відбулось на 32Вт.

Із проведених досліджень встановлено, що збільшення швидкості передачі не призвело до збільшення енергетичного споживання генератора напруги. Вибір орієнтації зразка в модуляторі з електрооптичним коефіцієнтом r_{ij}=39,7*10^{-12} м/В, дав змогу отримати зменшення енергоспоживання модулятора на 67,7%, у порівнянні із прямим зрізом (r_{ij}=3.4*10-12 м/В).

Література

1. М. Кайдан, В. Андрущак. Модель Розрахунку Енергоефективності для Електро- та Акустооптичних Пристроїв у Оптичній Транспортній мережі. In Proceeding of the I International Conference Advanced Information and Communication Technologies (AICT’2015) с.171-174.
2. Г.В. Колодезная. Оптические системы передачи. Учебное пособие. Хабаровск: Изд-во ДВГУПС, 2002. – 99с.
3. Franklin, Mark A., and Tilman Wolf. "Power considerations in network processor design." *Network Processor Design: Issues and Practices* 2 (2003): 29-50.
4. F. Idzikowski. Power consumption of network elements in IP over WDM network. TKN technical Reports Series – Berlin. – 2009.
5. П.С.Лопатина, В.В.Криштоп. “Електрооптический модулятор для волоконно-оптических линий связи”. Изв.Вузов.Приборостроение. – 2009. - Т.52. - №12. – с.67-71.
6. Andrushchak A.S., Mytsyk B.G., Demyanyshyn N.M., Kaidan M.V., Yurkevych O.V., Dumych S.S., Kityk A.V., Schranz W. Spatial anisotropy of linear electro-optic effect for crystal materials : II. Indicative surfaces as efficient tool for electro-optic coupling optimization // Optics & Lasers in Engineering.– 2009.–V.47, N.1. – P.24-30.

УДК 621.391

ОПТИЧНА НАДІЙНІСТЬ ВОЛОКОННО-ОПТИЧНИХ КАБЕЛІВ ЗВ'ЯЗКУ В РЕЗУЛЬТАТІ СТАРІННЯ

Харченко М.О., Каток В.Б.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: 9419xmo@ukr.net

Optical reliability of fiber optic cables as a consequence of their aging

This work suggests the short analysis of factors which deteriorate optical characteristics of glass fibre as a consequence of its aging. These factors should be considered as starting point in identifying processes that need to be accounted for to assure the optical performances of the manufactured and cabled fibers prescribed in G.65x series of International Telecommunication Union (ITU) Recommendations.

За 30 років комерційного використання оптичного кабелю, було ідентифіковано фактори, які виникають в результаті старіння скловолокна та погіршують його оптичні характеристики. Ці фактори повинні бути враховані при виготовлення кабельних волокон, стандартизованих в Рекомендаціях Міжнародного союзу електрозв'язку (МСЕ) серії G.65x, щоб гарантувати надійність їх роботи. Основна увага приділяється трьом видам впливу на оптичну надійність:

- втрати на вигинах (мікровигини і макровигини);
- хімічний вплив (водень є найбільш поширеним фактором);
- радіаційна чутливість.

Багато з випробувань з оптичним волокном і кабелем, наведених в документах IEC SC86A і ITU-T SG15 WP2, були розроблені для реалізації тривалої надійності оптичних кабелів. Випробування зосереджені на моніторингу оптичної надійності всіх волокон та на затуханні сигналів в волокнах в кабелі в цілому.

Якщо отримані результати тесту знаходяться в рекомендованих межах, оптичні кабелі повинні стабільно функціонувати впродовж прийнятного періоду часу (20-30 років) без значного погіршення якості передачі.

Втрати на вигинах розподіляються на два типи, втрата на мікровигинах та втрата на макровигинах. Простіше кажучи, макровигини — це видимі вигини радіусом в декілька міліметрів, а мікровигини — дуже дрібні вигини, радіус яких становить декілька мікрон і сумірні з довжиною оптичних хвиль. Вигини з'являються в багатьох місцях всієї довжини оптичних волокон і розрізнити макровигин від мікровигину часто може бути складно, особливо в області переходу між цими двома поняттями. Для одномодових волокон обидва ефекти викликають збільшення втрат зі збільшенням довжин хвиль, зокрема становлять загрозу довгим хвилям (в C- і L-діапазонах до 1625 нм) [1].

Втрата на мікровигині оптоволокна виникає в одномодовому світловоді, коли дрібні поперечні недоліки в конструкції волокна призводять до виведення енергії з основного режиму в багатомодовий режим з більшими втратами та випромінюючий режим. Значна втрата від мікровигину може виникнути навіть

коли його величина має розмір в нанометрах. Спектральна залежність втрати від мікровигинів варіюється залежно від осьового розподілу недоліків волокна. Мікровигини можуть стати результатом зміни температур, які спричиняють розширення та набухання захисного покриття волокон або кабельного матеріалу, що є реакцію на зовнішнє середовище. Волокна та кабелі є об'єктами навантажувальних випробувань впливу температурних змін, вологості, води та інших розчинів для передбачення роботи кабелю впродовж терміну експлуатації. Типові види тестів, стандартизовані Міжнародною електротехнічною комісією (МЕК), вказані в додатку VI.4 ITU-T G.Sup.40[3].

Другий фактор впливу на оптичну надійність – водень. Водень – це мала молекула, яка може легко розподілятися в структурі скла. Було виявлено, що коли волокна тривалий час знаходяться в атмосфері з високим вмістом водню, молекули водню можуть дифузіювати в волокна і викликати збільшення загасання на більш довгих хвилях (1300 і особливо 1500 нм), а коли концентрація водню в повітрі дуже мала, він може утворюватися всередині деяких кабелів в результаті розкладання пластикових матеріалів[2].

Водень може реагувати зі склом, щоб створити незворотні точки поглинання (тип 1), які додають оптичні втрати або інтерстиціальний молекулярний водень, який може бути присутнім в склі, також додає загасання (тип2). Обидва типи мають відношення до сучасних оптичних кабелів, оскільки вони можуть збільшувати загальне загасання оптичного кабелю.

Впроваджений водень (тип 2) є проблемою лише тоді, коли на оптичний кабель поширюється дія високого парціального тиску водню. Одним із застосувань, де цей тип водню становить загрозу це підводні кабелі. Оптичні кабелі, які використовуються глибоко під водою, понад 100 метрів нижче поверхні води, поміщають в герметичні пакети та найчастіше в труби з нержавіючої сталі, щоб запобігти виникненню поглинання 2 типу. Оптичні волокна, які застосовуються в мілководних кабелях глибиною менше ніж 100 м розширюється під впливом водню і цей вплив збільшується з глибиною. Вплив водню другого типу можна знищити, як тільки кабель витягти з води, водень розсіюється з кабелю і загасання повертається до норми [1].

Водень може реагувати з дефектами в матриці скла. Ці дефекти 1 типу найбільш очевидні в волокнах ITU-T G.652.B. Тривала дія водяної пари може привести до проникнення в волокна, які знаходяться у воді, гідроксильних іонів (OH), викликаючи втрату міцності і збільшення загасання [2]. У значній кількості ці дефекти можуть зробити оптичні кабелі непридатними до використання.

У 2001 році ITU-T ввели повний спектр волокна G.652.D. Ці волокна G.652.D відрізнялися від своїх попередників тим, що скло, яке пропускає світло стабілізується так, що при типових умовах розміщення, водневі дефекти 1 типу не утворюються в достатній кількості, щоб негативно позначитися на якості пропускання оптичного волокна. Сьогодні більшість оптичних волокон задовольняють цю специфікацію забезпечуючи більш надійне довгострокове оптичне функціонування. У разі, коли волокна G.652.D піддаються концентрації водню значно вище, ніж в звичайних умовах, то описані дефекти можуть утворюватися і погіршувати оптичну якість волокна.

Вплив ядерної радіації також впливає на оптичну надійність оптичного волокна. Опромінення легованих германієм оптоволокон радіоактивним випромінюванням може викликати дефекти в будові атомів скла, що призводить до збільшення загасання, викликане радіацією. Тестування радіації на сьогоднішній день проводять з великими дозами за короткі інтервали часу. Результати таких прискорених тестів використовуються для оцінювання збільшення згасання волокон за розрахований термін експлуатації під час опромінення на фоновому рівні. Оптичні кабелі масово застосовуються з 1977-го року і, як показав світовий досвід, радіаційний фон не впливає на показники згасання робочих кабелів за нормальних умов [1].

Очікуваний термін експлуатації оптичних волокон становить не менш 20-30 років. Метою випробувань на старіння є допомога кінцевому користувачеві прогнозувати оптичні властивості оптичного кабелю протягом усього терміну його служби. Ці тести перевіряють на циклічних умовах, що можуть виникати через зміни протягом року, локалізовані події, такі як вигини, а також погіршення характеристик протягом усього терміну експлуатації кабелю. Ряд тестів, які були розроблені перераховані в додатку VI.4 ITU-T G.Sup.40[3].

Багато з розроблених випробувань передбачені для циклічного проведення:

- Циклічний вплив температури на оптичне волокно та кабель;
- Циклічні випробування на вологостійкість оптичного волокна та кабелю;
- Випробування на макровигини оптичного волокна та кабелю;
- Випробування на руйнування оптичного кабелю.

У цих тестах є вимоги до гіршого випадку продуктивності при заданому наборі умов, які відповідають гіршому випадку експлуатаційних умов. Під час використання оптичного кабелю, очікується, що збільшення загасання буде меншим або дорівнює тим, які спостерігалися в цих тестах.

За 30 років використання оптичних кабелів та з прогнозом того, що будь-який деградаційний ефект подвоїться за наступні 30 років, ми можемо припустити, що малоймовірно, що окрім впливу водню, може виникнути ще якісь чинники погіршення оптичної продуктивності, які могли б призвести до втрати більш ніж декількох сотих дБ на кілометр за весь термін експлуатації оптичного кабелю. За нормальних умов прокладання та експлуатації оптичних кабелів, можна очікувати термінів їх експлуатації понад 30 років.

Література

1. Optical Fibre and Cable Reliability Guidelines. Supplement FCR to the ITU-T G-series Recommendations, ITU Geneva, February 2016.
2. Дэвид Бейли. Волоконная оптика. Теория и практика / Дэвид Бейли, Эдвин Райт. – М.: КУДИЦ-Пресс, 2008. – 320с.
3. ITU-T G-series Recommendations. Supplement 40, ITU Geneva, June 2010.

УДК 621.382

МУЛЬТИСЕРВІСНІ МЕРЕЖІ ДОСТУПУ НА БАЗІ АРХІТЕКТУРИ PON ДЛЯ КОТЕДЖНОЇ ЗАБУДОВИ

Федюшина Д.М., Каток В.Б.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: dfediushyna@gmail.com

MULTISERVICE NETWORK BASED ON PON ARCHITECTURE FOR COTTAGE BUILDINGS

The basic advantages and features of the deployment of multi-service network based on PON technology for cottage buildings are presented. Also there are mentioned some typical project deployment solutions for such of network and some examples of NG-PON service are listed.

Ринок котеджної нерухомості Київської області, та і України в цілому, активно розвивається. Нині зведення заміських котеджів стає прерогативою будівельних компаній. У розвинених країнах життя в передмісті давно стало повсякденною практикою для середнього класу, що, звичайно, чекає і Україну. Розуміючи це, очевидно, що зростатимуть і вимоги до мереж доступу згаданих котеджних містечок. В даній роботі було представлено рішення цієї проблеми.

Головна проблема, що стоїть перед операторами зв`язку: надання абонентам різних фізичних інтерфейсів, широкої смуги пропускання при мінімумі витрат. Пошуком рентабельного рішення в 1995 році почав займатись консорціум FSAN (Full Service Access Network), а у 2001 році – альянс EFMA (Ethernet in the first mile). Акцент діяльності обох асоціацій ставився на розвиток технології PON (Passive Optical Network).

Мережа PON – деревовидна архітектура, що передбачає передачу інформації по одному волокну на двох довжинах хвиль: 1550 нм (downstream) 1310 нм (upstream). На проміжних ділянках розміщуються пасивні оптичні розгалужувачі. Для розподілення смуги пропускання між абонентами використовується TDMA. У наш час розгортаються мережі 10G EPON, 10G GPON, 40 GPON, а також NG-PON. Для прикладу, у таблиці1. приведено перелік деяких послуг, що надаються при розгортанні мережі XG-PON.

Для передачі прямого та зворотного каналу використовується одне оптичне волокно, смуга пропускання якого розподіляється між абонентами динамічно, або ж використовується два волокна у випадку резервування.

Таблиця 1. Приклад послуг, що надаються при розгортанні мережі XG-PON

No.	Сервіс	Коментарі
1	Телефонія	VoIP
2		POTS
3	TV (real-time)	IPTV: сервіс доступний, використовуючи IP multicast/unicast
		Digital TV broadcasting: сервіс доступний, використовуючи накладання RF-відео (див. [ITU-T G.983.3], [ITU-T J.185] та [ITU-T J.186])
4	Виділені лінії	T1: швидкість 1.544 Mbit/s. Затримка основного сигналу має бути не більше 1,5 мс
5		E1: швидкість 2.048 Mbit/s. Затримка основного сигналу має бути не більше 1,5 мс
6	Високошвидкісний доступ до мережі Інтернет	UNI базується на Gigabit Ethernet
7	L2 VPN послуги	послуги Ethernet та ін.
8	IP послуги	L3 VPN, VoIP та ін.

Переваги архітектури PON:

- відсутність проміжних активних вузлів;
- економія оптичних прийомопередавачів у центральному вузлі;
- економія волокон;
- економія електроенергії;
- економія виробничих площ;
- економія каналізаційно-кабельних споруд;
- легкість підключення нових абонентів та зручність їх обслуговування (вихід з ладу одного вузла ніяк не впливає на роботу інших).

До перспективних можливостей розвитку мереж доступу в заміських котеджних містечках відносять:

- Більшість населення має середній чи високий рівень життя;
- Спостерігається потреба у цифровому телебаченні високої якості (а також додаткові функції цифрової телефонії);
- Такі котеджні забудови знаходяться недалеко від міст;
- Через приватні інвестиції операторів зв`язку для заняття сегменту ринку.

Для розгортання такого роду мережі типові проектні рішення передбачають використання уже готової інфраструктури:

- Мережі кабельної каналізації з прокладанням волоконно-оптичного кабелю в каналах зі встановленням оптичних муфт в оглядових пристроях;
- Використання опор ЛЕП з підвіскою діелектричного волоконно-оптичного кабелю та встановленням на них оптичних муфт.

Ділянка від розподільної абонентської муфти до оптичного абонентського терміналу, що встановлюється всередині котеджу називається ділянкою абонентської проводки. Допускається кілька варіантів проведення кабелю в котедж:

- Проведення через зовнішню стіну будівлі;
- Проведення з даху через трубостійку;
- Підземне прокладання з виходом на зовнішню стіну будівлі.

Як підсумок, можна зауважити, що перспектива розвитку оптичних широкосмугових мереж з доступом безпосередньо до приватних будівель малоповерхового будівництва дуже висока. Ринок котеджної нерухомості стрімко розвивається, це відкриває нові сегменти ринку для операторів зв`язку. Водночас із цим варто не забувати про такий же системний підхід та правила побудови оптичних мереж, що визначені для міських мереж. Це дозволить не лише забезпечити ефективність фінансового вкладу, але і якість послуг, що надаються населенню і, відповідно, довгострокову співпрацю.

Література

1. Стандарт ITU-T G.987.1. **10-Gigabit-capable passive optical networks (XG-PON): general requirements.**
2. Каток В.Б., Руденко І.Е., Ранський Є.Г. Однорог П.М. Під ред. Катка В.Б. Волоконно-оптичний зв`язок – К.: Логос, 2015.
3. Каток В.Б., Руденко І.Е. Під редакцією Катка В.Б. Волоконно оптичні кабелі зв`язку. – К.: Логос, 2013.
4. Каток В.Б., Ковтун А.С., Руденко И.Э. Оптика по высшим стандартам / – Сети и телекоммуникации, №11, 2004.

УДК 621.391

ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ GPON У МУЛЬТИСЕРВІСНИХ МЕРЕЖАХ ДОСТУПУ

Воронін Р.О., Каток В.Б.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: roma.voronin88@gmail.com

GPON technology usage in multiservice access networks

This paper provides a brief analysis and the benefits of GPON technology implementing. This fiber-optic technology is used in subscriber access networks and allows for low operating costs to build a network, covering the whole city at low cost of optical fibers, electrical energy and resources of wired telecommunications infrastructure.

Ринковий аналіз показує, що лише волоконно-оптичні кабелі мають потенціал для підтримки гігабітних швидкостей та передачі інформації на великі відстані, що мають місце в мережах доступу. FTTH (Fiber To The Home – волокно до домівки) мережі мають стати основним рішенням для мереж абонентського доступу і почати впроваджуватись ширше, щоб Інтернет-провайдери могли з легкістю надавати смугу пропускання, затребувану кінцевим користувачем. Нова архітектура FTTH формуватиме основу для майбутніх мереж доступу, які будуть задовольняти потреби абонентів в швидкостях доступу до ресурсів, контенті та сервісах впродовж довгих років в майбутньому [1].

Розвиток технології мультиплексування з розділенням по довжині хвилі (WDM), яка використовує одне волокно для вхідного та вихідного трафіку, став вдосконаленням для волоконно-оптичних технологій. Зрештою, ранні мережі FTTH типу «точка-точка» було замінено новим типом побудови мережі – «точка-многоточка», де одиночне волокно з'єднується з пасивними оптичними розгалужувачами, які розподіляють волокна до декількох абонентів. Ці пасивні оптичні мережі (PON – Passive Optical Network) можуть підтримувати розділення потоку з одного волокна у відношенні 1:64 і більше. Деякі PON мережі також включають додаткову накладену довжину хвилі для вхідного потоку, що забезпечує аналогові або цифрові телевізійні послуги користувачам [2].

Типові PON архітектури FTTH підтримують Ethernet підключення через спеціальний стандарт протоколу пасивної оптичної мережі. Одиночне волокно з оптичного лінійного терміналу (OLT) центрального офісу підключається до оптичних мережевих терміналів (ONT) або оптичних мережевих блоків (ONU), розташованих в приміщенні клієнта. Пристрій ONT, як правило, розташовується безпосередньо у домівці кінцевого користувача, в той час як пристрій ONU може розташовуватись в підвалі багатоквартирного будинку і бути загальним в користуванні для невеликої кількості абонентів [1].

Найбільш поширеними та використовуваними стандартами PON на сьогодні є EPON/GEPON (на основі стандарту IEEE 802.3ah) і GPON (ITU-T G.984). Стандарт EPON/GEPON використовує Gigabit Ethernet з симетричними швидкостями вниз і вгору. GPON було розроблено, щоб забезпечити більші downlink (вхідний потік) швидкості ніж uplink (вихідний потік) [3].

Рис. 1 GPON FTTH «точка-многоточка».

Явною перевагою PON мереж є той факт, що одне загальне оптичне волокно може використовуватись багатьма користувачами за допомогою використання недорогих пасивних оптичних розгалужувачів. В мережах GPON до 64 ONT можуть «розділяти» одне волоконне підключення до OLT. Це робить GPON привабливим рішенням для постачальників послуг, що бажають замінити мідні мережі на волоконно-оптичні, особливо в густозаселених міських районах [4].

Серед інших переваг та особливостей мереж GPON експерти виділяють:

- Стандартизованість – GPON являється стандартом ITU-T G.984 (клас B+);
- Робота на швидкостях 2,488 Гбіт/с вхідного потоку і 1,244 Гбіт/с вихідного потоку з можливістю гнучкого нарощування швидкості доступу;
- Практичне розділення волокна в співвідношенні до 1:64 (стандарт підтримує відношення до 1:128);
- Відстань між OLT і ONT/ONU може складати до 20 км, що дозволяє з легкістю задовольняти потреби цілого міста, використовуючи декілька OLT;
- GPON визначає якість обслуговування QoS і протоколи управління, необхідні для мультисервісних Triple-Play послуг в мережі доступу;
- Відсутність активного обладнання в мережі доступу, що дозволяє уникнути проблем з електромагнітними перешкодами чи блискавками;
- Зменшення кількості обладнання, оптичних волокон і виробничих площ в центральному офісі провайдера;
- Незначні витрати електроенергії на порт.

GPON призначена для забезпечення мультисервісних Triple-Play послуг (дані, відео та голос), а не тільки для високошвидкісного доступу в Інтернет.

Вона повністю доступна для клієнтів за рахунок підвищення ефективності використання смуги пропускання стандарту PON [4].

Нові стандарти, такі як 10-, 40- і 100-GPON, підвищують продуктивність мереж PON до 10, 40 і 100 Гбіт/с відповідно при збереженні сумісності з вже розгорнутими GPON мережами [G.987, G.989]. Сумісність різних типів і різних поколінь PON мереж забезпечується використанням різних довжин оптичних хвиль в системах. Для можливості використання в одній мережі обладнання різних постачальників вказані довжини хвиль стандартизуються в ITU-T.

На рисунку 2 показано пристрої ONT, розгорнуті в типовій мережі GPON, що забезпечує послуги Triple-Play для абонентів.

Рис. 2 Застосування GPON ONT в жилому приміщенні клієнта.

Встановлений в будинку ONT типу А забезпечує доступ в Інтернет з ПК через один зі своїх LAN портів. Інший LAN порт підключається до IP-TV приставки, яка в свою чергу підключається до телевізора для забезпечення IP-TV відео. Стандартний аналоговий телефон підключається до RJ-11 порту, який дозволяє робити VoIP виклики через Інтернет. Встановлений в іншому будинку ONT типу В підтримує ті ж Інтернет і VoIP послуги, але цей ONT також забезпечує доступ в Інтернет для ноутбука, планшета чи смартфона через Wi-Fi з'єднання 802.11n. Окрім цього такий ONT надає послугу кабельного телебачення безпосередньо до телевізора через радіочастотне коаксіальне з'єднання [5].

Поточні та майбутні потреби в швидкостях доступу в Інтернет приводять до широкого розгортання FTTH технологій. Серед цих технологій GPON забезпечує гнучкість та цінові переваги, що дозволяє провайдерам вигідно надавати послуги для своїх абонентів.

Література

1. Булл Е.К. Довідник з мереж FTTH, 5-е видання – Connolly Communication, 2012. – 119 с.
2. Фриман Р. Волоконно-оптические системы связи / Пер с англ. Слепов Н.Н. – М.: Техносфера, 2007. – 514 с. – ISBN 978-5-94836-154-3.
3. Роблек Е. «FTTC, FTTH, FTTB Access», Посібник – 2011. – 38 с.
4. Каток В.Б., Солодовник О.І. Волоконно-оптичні мережі доступу по технології FTTx. – К: 2010.
5. Стандарт ITU-T G.984.1. Gigabit-capable passive optical networks (GPON): Загальні характеристики.

УДК 681.7.068

ПОБУДОВА МЕРЕЖІ FTTH НА ОСНОВІ МІКРОТРУБЧАТОЇ КАНАЛІЗАЦІЇ ДЛЯ РАЙОНІВ ІНДИВІДУАЛЬНОГО ЖИТЛА

Сапа Т.І.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: sapatatiana@gmail.com

Building of a network FTTH on the basis of micro tubular sewerage for the districts of individual housing

Describes how to connect the optical fiber on the concept FTTH using the method of injection of fiber in micro-tubes for areas of low-rise buildings. Connection example for low-rise buildings.

Мережі доступу є найбільш витратною ланкою операторських мереж зв'язку. У наш час на ділянці доступу використовують переважно мідні кабелі (виті пари). Їх канальна ємність та пропускна здатність не дозволяє в повністю реалізувати сучасні мультисервісні послуги. Для надання нових мультисервісних послуг потрібна смуга пропускання, яка зазвичай ширша, ніж та, яку можуть забезпечити технології, які існують зараз в мідно-кабельної інфраструктури. Тому, щоб організувати доступ до широкосмугових послуг найбільш ефективною є побудова волоконно-оптичної кабельної інфраструктури.

Ідея використання волоконно-оптичних ліній зв'язку (ВОЛЗ) не нова. Вона реалізується в рамках концепції FTTx (Fiber to the x - «волокно до х», де х-точка присутності волокна). Є багато різновидів даної концепції, в даному випадку розглянемо найбільш перспективну технологію FTTH - Fiber To The Home (доведення ВОЛЗ до квартири);

Доступ зв технологією FTTH є найбільш витратним, але в той же час і найбільш затребуваним, а значить і перспективним, серед всіх типів доступу FTTx.

Структура FTTH передбачає максимальне використання оптичних технологій, при якій оптичний мережевий термінал знаходиться в квартирі користувача і з'єднується короткими кабелями з кінцевими пристроями - телефоном, комп'ютером, телевізором і т.д.

Технологія FTTH заснована на методі пневмопрокладки, не використовується в Україні, але популярна в Європі і США як найбільш гнучка і перспективна з існуючих технологій прокладки ВОЛЗ.

Основні її переваги:

- Малий діаметр захисних поліетіленових труб;

- Можливість розгалуження без застосування оптичного зварювання, тому що відгалужуються не волокна, а мікротрубки, в яких ще немає ОК.

Використання даної технології дозволяє в міру необхідності збільшувати число волокон в лінії без ризику пошкодження сусідніх кабелів, тому що повітряний тиск подається тільки в порожню мікротрубку і в кожної мікротрубці знаходиться не більше одного кабелю;

- Можливість відгалуження безколодязним способом, тому що відгалужувальні муфти вкладаються безпосередньо в грунт;

- Немає необхідності в прокладанні резервних оптичних модулів які можуть знадобитися пізніше, вони легко прокладаються при необхідності в уже прокладені мікротрубки за незначний відрізок часу, що значно може понизити початкові витрати;

- Можливість розширення мережі без необхідності проведення земельних робіт, які завжди вимагають і вкладень і додаткових погоджень, розширення відбувається без зупинки експлуатації мережі;

- Широкий вибір кількості і розмірів каналів дає можливість прийняття оптимального рішення.

Мікротрубчата каналізація у малоповерховій забудові.

Розподільна частина мережі FTTH це деревоподібна структура, стовбур якої починається в розподільчому вузлі, а гілки закінчуються у абонентів. Подібну топологію має і мікроканалізація. Стовбури – це багатотрубочні кабелі, що проходять уздовж вулиць, від яких в декількох місцях до будинків або до дроп-вузлів відходять гілки - однотрубочні кабелі.

Покажемо підхід трубка в будинок. Новизна технології в тому, що її ще не використовують в Україні. Покажемо приклад, можливого підключення. По трубці можна підвести одне або кілька волокон. Уздовж вулиць прокладаються кабелі з великою кількістю трубок (12-24), при цьому обслуговуючих оглядових пристроїв може не бути зовсім.

Однотрубчатий кабель або трубка, відведена в період будівництва до абонента перед його ділянкою, може бути заглушена і залишатися в грунті. На етапі підключень абонентські трубки докладаються. Волокна доводяться методом пневмопрокладки до абонентської розетки (трубки прокладаються і по дому, але у виконанні LSZH). Це все переваги, недоліки такі: великі витрати на етапі будівництва (велика кількість багатотрубчатих кабелів), потрібно кожен раз привозити громіздке обладнання при підключенні абонентів поодинці і потрібне проведення одиночних сварок волокна (або стикувань). Середня довжина абонентського кабелю (модуля) при цьому становить кілька сотень метрів.

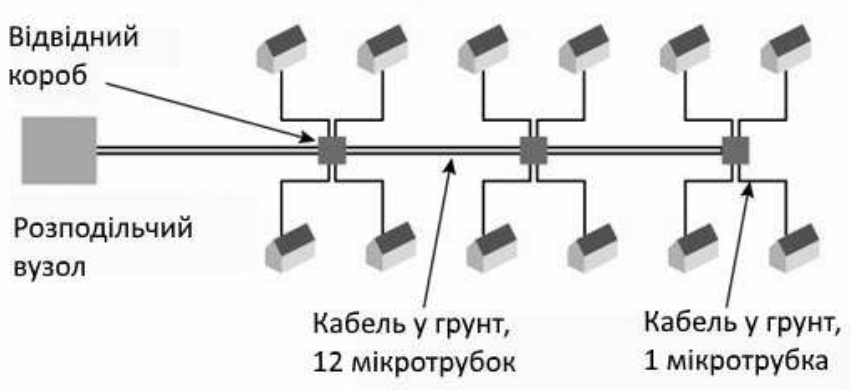


Рис. 1. Топологія прокладання мікротрубок від розподільчого вузла до будинку абонента.

В останні роки збільшуються тенденції до персоналізації отримання даних для абонентів широкосмугових мереж і підвищення їх надійності. Тому має місце розширення використання мереж Ethernet FTTH, PON. Дані технології становлять великий інтерес для сервіс-операторів і мають перспективи розвитку, тому що вони дозволять персоналізувати послуги та нададуть широкі можливості для збільшення смуги пропускання і передачі будь-якої інформації в тому числі передачу голосу, трансляцію відео високої якості, які набувають в останні році популярність інтерактивних керованих послуг.

Мікроканалізація - це ефективний і економічно виправданий спосіб створення підземних мереж FTTH, який використовує перевагу оптичного волокна - його мініатюрність. Мікроканалізація вимагає певної культури будівництва і освоєння нових мініатюрних будівельних механізмів і приладів. Особливо ефективна мікроканалізація в житлових кварталах з малоповерхової забудовою.

Література

1. Е.Гаскевич, І.Петренко Мікротрубчата каналізація для мереж FTTH (Первая Миля №4,2012).
2. Бубліченко Н. Широкосмуговій доступ в рамках архітектури FTTx: ефективні рішення компанії "СТР". - Журнал "Первая миля", № 5-6, 2010.
3. Гаскевич Е., Петренко І., Убайдуллаев Р. Волоконно-оптичні мережі доступу для районів малоповерхової забудови. - Вісник зв'язку, 2011, №4.
4. Гаскевич Е. Мережі PON для районів індивідуальної та малоповерхової житлової забудови. - Первая миля, 2012 №1.

УДК 621.38

ИССЛЕДОВАНИЕ ПОМЕХОУСТОЙЧИВОСТИ МОНОИММИТАНСНОГО ЛОГИЧЕСКОГО R-ЭЛЕМЕНТА «И»

Филинюк М.А., Лищинская Л.Б., Стахов В.П.
Винницкий национальный технический университет, Украина
E-mail: vladstakhov@mail.ru

Research of monoimmitance logic R-element «AND» noise stability.

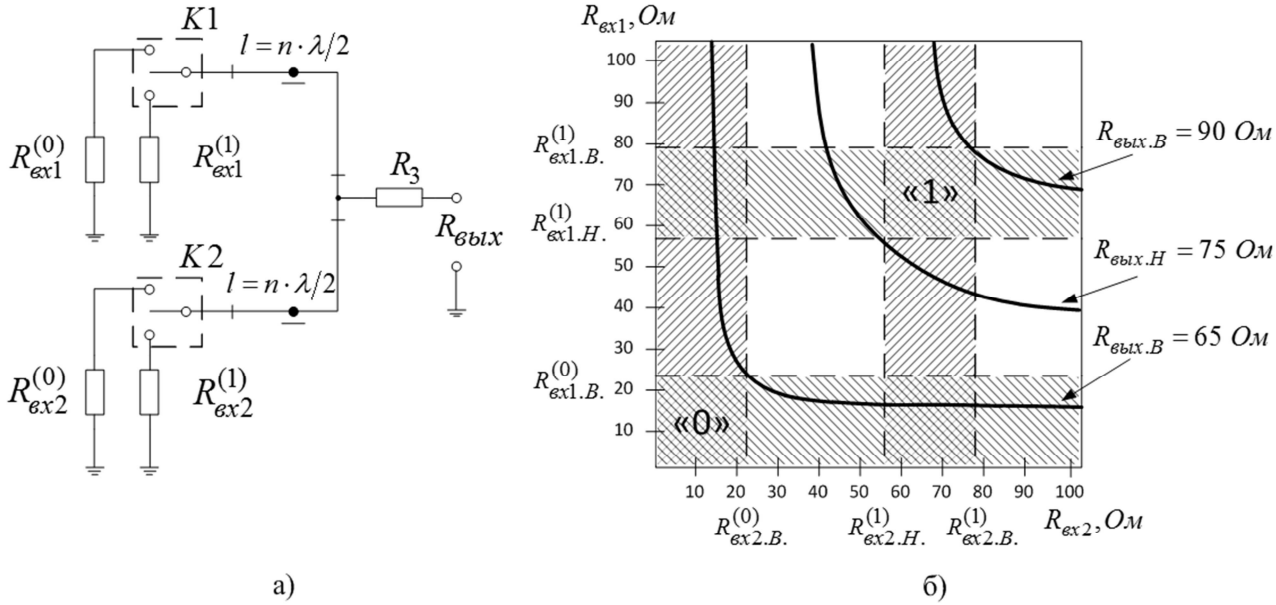
The bases of construction of R-monoimmitance logic element "AND" and results of researching of destabilizing factors effect on the characteristics of the logical monoimmitance R-element "AND" such as the instability of the wave resistance of the transmission line, the emergence of the transmission line segments length and the emergence of parasitic reactance in the input immitance is presented.

Одной из разновидностей радиочастотных логических элементов являются иммитансные логические элементы, которые используют в качестве информационного параметра характер или величину иммитанса [1,2]. Использование иммитанса позволяет существенно повысить помехоустойчивость и энергетическую эффективность логического элемента [3].

Иммитансные логические элементы могут использовать в качестве информационного параметра резистивный, индуктивный или емкостной иммитанс, а также их комбинации. При одновременном использовании нескольких видов иммитанса логические элементы называются мультииммитансными, а при использовании одного типа иммитанса - моноиммитансными логическими элементами [4]. Для практического использования более целесообразными являются моноиммитансные логические элементы, использующие один информационный параметр, например, только активное сопротивление - (R-элемент), емкостной иммитанс - (C-элемент) или индуктивный иммитанс - (L-элемент) [5]. Моноиммитансные логические элементы имеют высокое быстродействие и энергетическую эффективность, но меньшую помехозащищенность, чем мультииммитансные логические элементы. Оценка помехозащищенности и методов ее повышения требуют дополнительных исследований.

В данном докладе решается задача обоснования схемы моноиммитансного логического R-элемента «И», разработка его математической модели и предлагаются результаты исследования работы моноиммитансного логического R-елемента «И» в диапазоне изменения дестабилизирующих факторов.

Электрическая схема возможного варианта реализации моноиммитансного логического R-элемента «И» представлена на рис.1а.



а) б)

Рис. 1 Электрическая схема (а) и иммитансная передаточная характеристика (б) моноиммитансного логического R-элемента "И" (на схеме К1 і К2 - условные переключатели).

Выходное активное сопротивление схемы при условии, что длина всех соединительных отрезков линии передачи $l = n \cdot \lambda/2$, где $n = 0,1,2...$, λ – длина электромагнитной волны в линии передачи, равно:

$$R_{вих} = R_3 + \frac{R_{вх1} R_{вх2}}{R_{вх1} + R_{вх2}}, \tag{1}$$

где $R_{вх1}$ и $R_{вх2}$ - резистивные импедансы, определяющие входные логические уровни.

Уравнение (1) является математической моделью идеального моноимитансного логического R-елемента «И» и описывает его иммитансную передаточную характеристику, которая представляет собой в координатах $R_{вх1}$ и $R_{вх2}$ семейство равносторонних гипербол, положение которых может регулироваться величиной резистора R_3 (рис. 1б).

В реальном моноиммитансном логическом элементе выходной иммитанс $Z_{вых}$ связан с выходными импедансами $R_{вых1}$ и $R_{вых2}$ отрезков l_1, l_2 линии передачи:

$$R_{вых1} = Z_0 \cdot \frac{R_{вх1}/Z_0 \cdot (1 - X_{вх1}/Z_0 \cdot tg\beta) + R_{вх1}/Z_0 \cdot tg\beta \cdot (X_{вх1}/Z_0 + tg\beta)}{(1 - X_{вх1}/Z_0 \cdot tg\beta)^2 + (R_{вх1}/Z_0 \cdot tg\beta)^2}, \tag{2}$$

$$R_{вых2} = Z_0 \cdot \frac{R_{вх2}/Z_0 \cdot (1 - X_{вх2}/Z_0 \cdot tg\beta) + R_{вх2}/Z_0 \cdot tg\beta \cdot (X_{вх2}/Z_0 + tg\beta)}{(1 - X_{вх2}/Z_0 \cdot tg\beta)^2 + (R_{вх2}/Z_0 \cdot tg\beta)^2}, \tag{3}$$

где $X_{вх1}$ и $X_{вх2}$ - реактивные входные импедансы, $\beta = 2\pi l/\lambda$ - фазовая постоянная; Z_0 - волновое сопротивление отрезков линии передачи.

С учетом (2) и (3) выходная активная составляющая импеданса моноиммитансного реального логического R-элемента «И» описывается выражением:

$$R_{вых} = R_3 + \frac{(R_{вых1})^2 \cdot R_{вых2} + R_{вых1} \cdot (R_{вых2})^2 + R_{вых1} \cdot (X_{вых2})^2 + R_{вых2} \cdot (X_{вых1})^2}{(R_{вых1})^2 + 2 \cdot R_{вых1} \cdot R_{вых2} + (R_{вых2})^2 + (X_{вых1})^2 + 2 \cdot X_{вых1} \cdot X_{вых2} + (X_{вых2})^2}. \quad (4)$$

Аналогичным образом рассчитываются и реактивные составляющие импеданса схемы.

Из анализа выражений (2-4) следует, что основными дестабилизирующими факторами являются:

- нестабильность волнового сопротивления Z_0 отрезков линии передачи;

- погрешность, связанная с изменением длины отрезка линии передачи Δl;

- появление во входных импедансах $Z_{вх1}$ и $Z_{вх2}$ паразитных реактивных составляющих $X_{вх1}$ и $X_{вх2}$.

Для сравнительной оценки помехоустойчивости иммитансного логического элемента использованы коэффициенты помехоустойчивости выходного активного импеданса $R_{вых}$: от нестабильности волнового сопротивления Z_0 отрезков линии передачи $\Upsilon_{Z_0} = 1 \Big/ \left(1 + \left| S_{Z_0}^{X_{Lвих}} \right|\right)$; от появления паразитных входных составляющих во входных импедансах $\Upsilon_Q = 1 \Big/ \left(1 + \left| S_{X_{вх}}^{X_{Lвих}} \right|\right)$; от погрешности длины отрезка линии передачи $\Upsilon_{\Delta l} = 1 \Big/ \left(1 + \left| S_{\Delta l}^{X_{Lвих}} \right|\right)$, где $S_{Z_0}^{R_{вих}} = \partial R_{вих} \cdot Z_0 / \partial Z_0 \cdot R_{вих}$, $S_{X_{вх}}^{R_{вих}} = \partial R_{вих} \cdot X_{вх} / \partial X_{вх} \cdot R_{вих}$, $S_{\Delta l}^{R_{вих}} = \partial R_{вих} \cdot \Delta l / \partial \Delta l \cdot R_{вих}$ - чувствительности выходного активного импеданса от вышеперечисленных параметров.

Для достижения большей помехоустойчивости логического элемента рекомендуется использовать входные импедансы с сопротивлением реактивных составляющих не более чем 10 Ом, обеспечить величину погрешности, связанную с изменением длины отрезка линии передачи Δl на уровне не более чем 1 мм на частоте 10 ГГц.

Литература

1. Ліщинська Л. Б. Імітансна логіка / Л. Б. Ліщинська, М. А. Філинюк // Інформаційні технології та комп'ютерна інженерія. — 2010. — No. 2. — с. 25–31.
2. Microwave immitance logical elements / L.B. Lishchynska, N.A. Filinyuk, R.Y. Chekhmestrouk, Y.S. Rozhkova – 22st International Crimean Conference: Microwave and Telecommunication Technology, CriMiCo 2012. – Sevastopol, Ukraine. – 10-14 September 2012. - P. 137-138.
3. Ліщинська Л. Б. Оцінка основних параметрів імітансних логічних елементів / Л. Б. Ліщинська // Інформаційні технології та комп'ютерна інженерія. - 2011. - № 3. - С. 45-52.
4. Filinyuk N. A. Monoimmittance logic R-elements / Filinyuk N. A., Lishchynskaya L.B., Voycekhovska O.V., Stakhov V. P. // П'ята міжнародна науково-практична конференція "Інформаційні технології та комп'ютерна інженерія" - Івано-Франківськ – Вінниця, 27-29 травня, 2015 р.
5. Филинюк Н.А. Моноиммитансные логические RLC-элементы / Н.А. Филинюк, Л.Б. Лищинская, Е.В. Войцеховская, В.П. Стахов // Вістник Хмельницького національного

університету, № 3. – 2015р. – с.117-121.
УДК 621.3

БУДУЩЕЕ СПУТНИКОВОГО ИНТЕРНЕТА

Тимченко И.О., Сундучков К.С.
Институт телекоммуникационных систем НТУУ «КПИ», Украина
E-mail: iratim4enko@gmail.com

THE FUTURE OF SATELLITE INTERNET

In the paper the new frequency band for satellite broadcasting, called Ka-band has been reviewed. Advantages, disadvantages, and the principle of satellite operation within the specified range were presented. Future prospects of its development and application for broadband access to the Internet were discussed. The new Ka- and previously used Ku-band were compared. Examples of the new generation of satellites, using Ka-band, as well as some parameters HTS-systems were shown.

Современный мир живет в эпоху, называемую “веком информационных технологий”. Каждый из нас имеет дело с огромным потоком данных, который необходимо получать и обрабатывать. На сегодняшний день существует много различных технологий и устройств, которые обеспечивают нас всесторонним доступом к любой информации.

Но существуют места и условия, когда доступ к средствам связи весьма затруднен. Люди не могут пользоваться, например, таким привычным для нас Интернетом. Данная проблема приобретает глобальных характер, когда речь идет о учебных учреждениях или объектах государственной важности.

Именно в таких случаях актуальным видом коммуникаций является спутниковая связь.

В современных космических системах начинается исследование и применение нового частотного Ка-диапазона и нового поколения спутников высокой пропускной способности (HTS).

Принцип работы спутников Ка-диапазона заключается в использовании группы точечных лучей. Каждый из них покрывает заданную зону и имеет полосу частот более 100 МГц.

HTS-спутники достаточно долговечны (десятилетия). Они поддерживают типы модуляции с большим коэффициентом модуляции, например, 32APSK. Системы HTS работают в Ка-диапазоне и применяют многолучевую технологию, обеспечивающую большую суммарную пропускную способность (в 40 раз) в сравнении с обычно применяемыми диапазонами Ku и C.

Для организации связи со спутниками прямой абонентский канал занимает полосу частот 19,7–20,2 ГГц (вниз), а для обратного канала выделена полоса 29,5–30 ГГц (вверх).

Ка-диапазон имеет свои преимущества и недостатки. Он не является оптимальным для всех сервисов и речь не идет о том, что он вытеснит применение Ku-диапазона. На некоторых современных спутниках применяются частично Ка-, Ku-, С- и даже L-диапазоны.

Спутники Ка-диапазона повторно используют частоты. Это изрядно экономит частотный ресурс по сравнению с ранее используемыми Ku и С диапазонами. Так обеспечивается большая скорость (до 20 Мбит/с для конечного пользователя) по более низкой цене. Количество обслуживаемых абонентов составляет от 100 тысяч до 1 млн.

Стоимость Ка-спутника дороже в 2-3 раза чем спутник Ku-диапазона, но стоимость на бит информации существенно меньше, поэтому в конечном варианте использование Ка-спутников оказывается дешевле. Еще одно достоинство - это меньшие размеры приемных антенн.

Но Ка-диапазон имеет ряд недостатков. Например, большое затухание при плохих погодных условиях. Поэтому необходимо более эффективно компенсировать это затухание. Также сложно организовывать земной сегмент. Требуются высокая производительность и доступная цена.

Перспектива использования новых спутниковых технологий. HTS-инновации имеют применение уже сегодня. Например, спутник Jupiter 1 (переименованный в EchoStar 17), который использует технологию HTS JUPITER. В зоне его покрытия - территория Северной Америки. Данный космический аппарат использует 60 точечных лучей. С их помощью обеспечиваемая пропускная способность составляет больше 100 Гбит/с. Этот спутник предоставляет услуги ШПД в Интернет почти 2 млн. абонентам.

Также один из первых HTS-спутников KA-SAT. В его зоне покрытия вся территория Украины (10 лучей) и др. континенты. Он использует всего 82 луча, обслуживая корпоративных клиентов. Общая пропускная способность 70 Гбит/с. Предполагаемая скорость 10 Мбит/с. Луч №68 данного космического аппарата покрывает город Киев, зона покрытия этого луча представлена на рис.1.

К 2016 году планируется запуск спутников нового поколения с пропускной способностью до 400 Гбит/с.

Я считаю, что подобные инновации очень актуальны для современности. Эти достижения могут быть полезны для других новшеств. Например, проект компании Cisco “Интернет во всем”. Для его реализации применение новых технологий спутниковой связи может быть просто необходимым и незаменимым.

Или же HTS-спутники с Ка-диапазона можно применить для доступа к сети Интернет мобильных терминалов, которые движутся по автобану или в железнодорожном экспрессе со скоростями до 300 км/час. Суммарная пропускная способность должна составлять 24 Гбит/с, количество обслуживаемых абонентов достигать 200, а необходимая скорость для конечного пользователя составляет 10-12 Мбит/с.

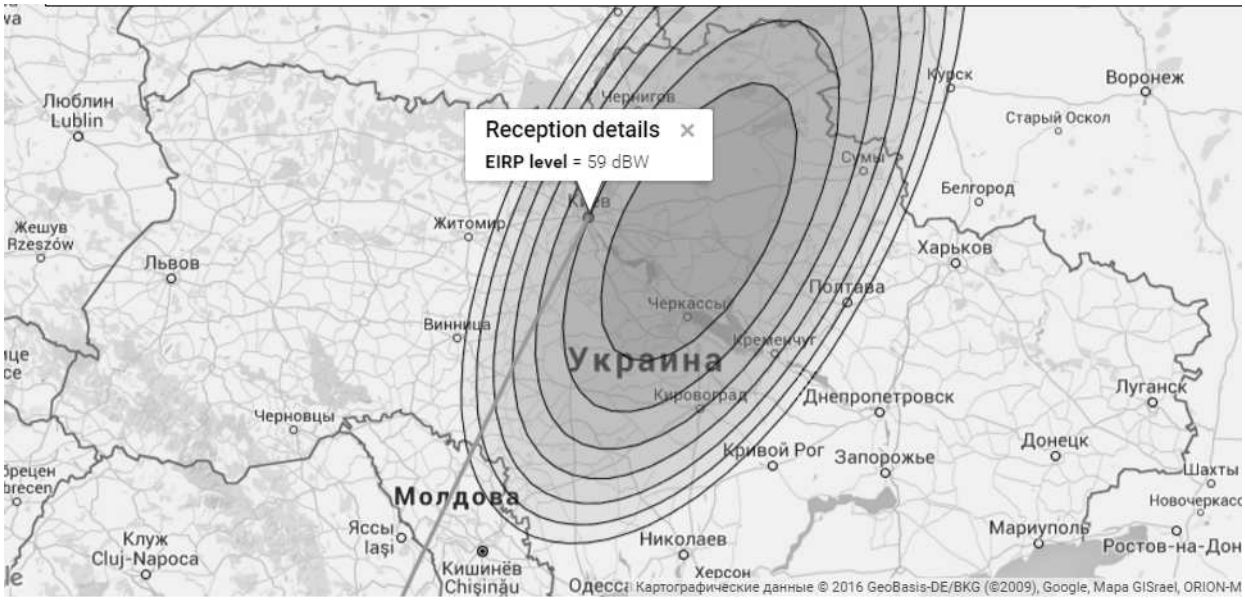


Рис. 1 Зона покрытия луча №68 спутника Ka-Sat.

Заключение. С каждым днем информации становится все больше и больше. Потребность в доступе к данным с любой точки мира возрастает. И иногда спутники - это единственный доступный вид коммуникаций.

Рассмотренные HTS-спутники, которые используют Ка-диапазон, имеют внушительную пропускную способность и финансовую экономичность. И это обеспечивает дальнейшее широкое применение данных спутников в корпоративных и коммерческих сетях, для сетей сотовой связи и интернет-провайдеров.

Литература

1. Георгий Башилов (2011). Журнал сетевых решений/Телеком. http://www.lanmag.ru: Ка-смические скорости. с.26-31.
2. Ben Pawling, Harris CapRock and Keith Olds, Harris Government Communications (Aug2013). Microwave Journal Freaquancy Matters.. 8th ed. http://www.microwavejournal.com/: Separating Fact from Fiction: HTS Ka- and Ku-Band for Mission Critical SATCOM. p22.
3. Константин Ланин (2015). Специальный выпуск "Спутниковая связь и вещание". 6th ed. РА "Лидер", Россия: Спутники высокой пропускной способности. стр.22-23.
4. Дорон Элинав (2013). Специальный выпуск "Спутниковая связь и вещание". 6th ed. "Триумф Медиа", Россия: Достоинства и перспективы Ка-диапазона. стр.36-37.

УДК 621.391

ДОСВІД ВИКОРИСТАННЯ ПРОГРАМНОГО КОМПЛЕКСУ LABVIEW У НАВЧАЛЬНОМУ ПРОЦЕСІ ТА У НАУКОВИХ ДОСЛІДЖЕННЯХ

Парфенюк В.Г.
Житомирський військовий інститут імені С.П. Корольова
E-mail: strob243@gmail.com

Experience of using of LabVIEW software complex in educational process and in research

The report provides experience of using of LabVIEW software system in the educational process in the study of digital radio transmission of information and in research. The advantages of this software system in the development of virtual laboratory devices and setting virtual physics experiment are presented.

У доповіді наводиться досвід використання програмного комплексу LabVIEW у навчальному процесі при вивченні цифрових радіосистем передавання інформації та у наукових дослідженнях. Показано переваги даного програмного комплексу для розробки віртуальних лабораторних установок та постановки віртуального фізичного експерименту.

Бурхливий розвиток цифрових телекомунікаційних технологій, зокрема цифрових радіосистем передавання інформації вимагає, підвищення рівня теоретичної та особливо практичної підготовки випускників профільних вузів.

Сучасні цифрові радіосистеми передавання інформації та їх пристрої відрізняються не тільки високою складністю схемотехнічної реалізації, а і складністю програмних додатків, які є невід'ємними складовими цифрових систем. Вони описуються значною кількістю параметрів та характеристик, які необхідно визначати з високою точністю за досить малий проміжок часу. Тому експериментальне дослідження таких пристроїв в умовах сучасного технічного вузу виявляється досить складним завданням. Ця складність багато в чому пов'язана із недоступністю для вузів сучасного телекомунікаційного обладнання та вимірювальних приладів через їх високу вартість та недостатнє державне фінансування.

Застосування інформаційних технологій для розробки лабораторного практикуму дозволяє подолати вищезгадані труднощі. Використання

інформаційних технологій дає можливість організувати проведення лабораторних робіт на новому, більш високому рівні, підвищити наочність отриманих результатів, поглибити їх розуміння, а також простежити процес перетворення сигналів та визначити основні закономірності їх обробки.

Сучасний лабораторний фізичний практикум допускає наявність автоматизованих лабораторних установок, у яких результати вимірів відображаються в режимі реального часу на екрані комп'ютера в найбільш зручній для аналізу формі, проводиться автоматизована математична обробка результатів з апроксимацією отриманих експериментальних залежностей у рамках існуючих фізичних моделей.

Сьогодні існує значна кількість програмних продуктів, орієнтованих на математичне моделювання пристроїв обробки сигналів: Micro-Cap, Matlab, Mathcad, Designlabn, Aplac, System View та ін. Однак, на наш погляд, лише програмний комплекс LabVIEW (Laboratory Virtual Instrument Engineering Workbench) найбільшою мірою враховує специфіку навчального процесу [1, 2]. Даний програмний комплекс спільно з додатковими модулями формування та обробки сигналів становить собою ефективний засіб створення лабораторних робіт для студентів, які мають на меті вивчення властивостей і характеристик різного виду радіосигналів та способів їх обробки.

Перевагами програмного комплексу LabVIEW є:

- висока швидкість засвоєння та зручний інтерфейс користувача, що дозволяє зосередитися на реалізації проекту, алгоритмах і методах обробки, а не на вивченні складної мови програмування;

- спрямованість на розв'язання питань розробки засобів вимірювальної техніки;

- наявність у пакеті вбудованих віртуальних контрольно-вимірювальних приладів;

- велика номенклатура програмних і апаратних інструментів, необхідних для збору, обробки, візуалізації та реєстрації вимірювальної інформації;

- наявність засобів моделювання як аналогових, так і цифрових вузлів;

- можливість створення на базі програмного забезпечення вимірювально-обчислювальних комплексів;

- доступність придбання програм;

- високий ступінь наочності, що підвищує інтерес до навчання, робить його більш доступним і міцним.

LabVIEW є графічною системою програмування, що використовує функціонально-логічний принцип розробки та графічного представлення

алгоритмів програм. LabVIEW легко опановується користувачами ПЕОМ, що не мають великого досвіду програмування. Програма на LabVIEW більш наочна, простіше модифікується та налагоджується, швидше розробляється.

Беззаперечною перевагою LabVIEW є також те, що розроблювачем програми для ПЕОМ може бути сам розробник завдання – викладач, інженер, студент.

Моделі сигналів, реалізовані з використанням додатків LabVIEW, сприяють вивченню їх структури, аналізу впливу шумів і фільтрації, їх спектральних та часових характеристик. Використання Labview надає можливість не тільки реалістично моделювати сигнали та пристрої їх обробки, але і досліджувати зміни їхніх параметрів на результати демодуляції та декодування, виявляти причини появи похибок і досліджувати методи їх зменшення, у тому числі із застосуванням завадостійкого кодування. Слід зазначити, що лабораторні комплекси можуть розроблятися як повністю віртуальними, так і у поєднанні з реальним лабораторним устаткуванням.

У доповіді демонструється декілька віртуальних лабораторних установок, розроблених із використанням програмного комплексу LabVIEW та модуля LabVIEW Modulation Toolkit, та результати проведення лабораторних робіт із їх застосуванням.

У доповіді розглядаються також питання постановки віртуального фізичного експерименту з використанням програмного комплексу LabVIEW та додаткових модулів, перевага у застосуванні якого полягає в простоті підготовки експерименту, високому ступені його наочності та доступності для викладача, який не має навиків програмування. Постановка під час навчальних занять такого експерименту дозволяє відтворити фізичні явища, що складно зробити в реальному лабораторному експерименті, урахувати його багатоваріантність. Показано, що впровадження віртуального фізичного експерименту на базі LabVIEW дозволяє суттєво спростити розуміння студентами фізичних процесів формування та обробки сигналів.

Література

1. Трэвис Д. LabVIEW для всех / Д. Трэвис, Д. Кринг. - М.: ДМК пресс, 2011. - 904 с.
2. Евдокимов Ю. К. LabVIEW для радиоинженера: от виртуальной модели до реального прибора/ Ю. К. Евдокимов, В.Р. Линдваль, Г.И. Щербаков. -М. : ДМК пресс, 2010. - 400 с.

УДК 378.147.111

ТЕХНОЛОГІЇ «ІНТЕРНЕТУ РЕЧЕЙ» - ПІДГОТОВКА ФАХІВЦІВ АКТУАЛЬНО В ЧАСІ

Могильний С. Б.
Радіотехнічний факультет НТУУ «КПІ», Україна
E-mail: isearch@ukr.net

Technology "Internet of Things" – timely specialist training

The analysis of the reality of the introduction of new technologies and evaluation terms of implementation to train specialists in accordance with the needs of today.

Вислів «Інтернет речей» заполонив медіапростір: одні переконують, що нова технологія зробить революцію в Інтернеті, інші більше акцентують увагу на тих небезпеках, які несе її впровадження. Спробуємо зробити аналіз реальності впровадження нової технології та оцінити терміни цього впровадження, щоб здійснювати підготовку фахівців, відповідно до запитів сьогодення.

Інтернет речей (англ. Internet of Things, IoT) - концепція обчислювальної мережі фізичних об'єктів («речей»), оснащених вбудованими технологіями для взаємодії об'єктів один з одним або з зовнішнім середовищем, яка розглядає організацію таких мереж без необхідності участі людини в частині дій та операцій.

Перш ніж починати підготовку спеціалістів з нових технологій, необхідно отримати відповідь на декілька питань: коли технологія вийде на «плато продуктивності», чи відповідає дана технологія нашим науковим напрямкам та спеціальності, наскільки реально вона буде втілена в життя і які ресурси наявні та необхідні додатково для підготовки спеціалістів.

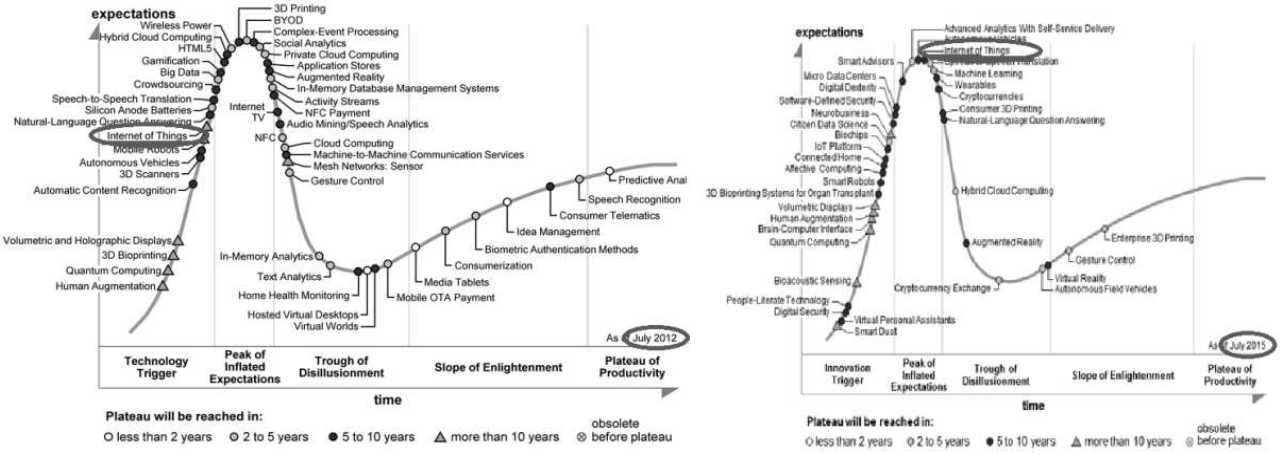


Рис. 1 Порівняння готовності нових технологій (2012 і 2015 роки).

Згідно прогнозів аналітичної фірми Gartner [1,2] вже через 5 років можна очікувати вихід технології на «плато продуктивності» і є тенденція до скорочення цього терміну (рис. 1).

Розглядаючи екосистему IoT [3] (рис.2), однозначно можна зробити висновок про відповідність технологій спеціальності «Телекомунікації та радіотехніка».

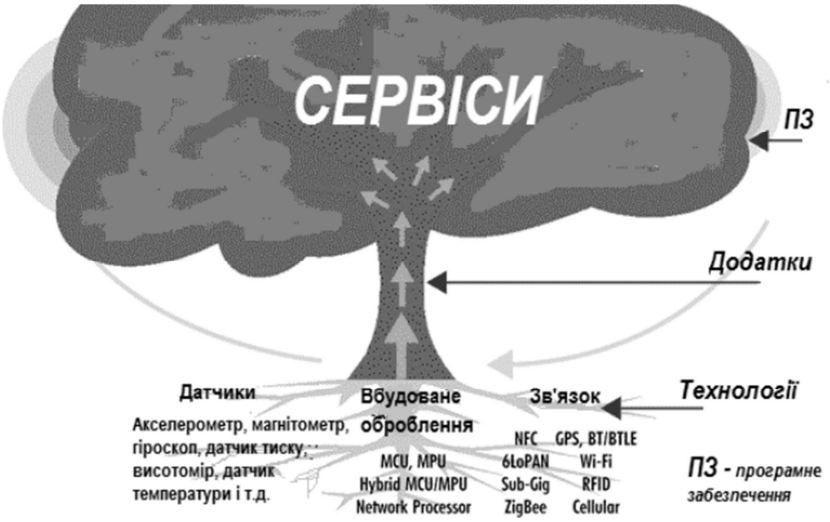


Рис. 2 Екосистема Інтернету речей.

Про реальність втілення в життя нової технології можна судити, якщо проаналізувати, хто розвиває її сьогодні і наскільки багато фінансів вже вкладено в дослідження та впровадження.

Основні прихильники нової технології: Cisco (Cisco IoT Services Portfolio – портфель сервісів для IoT), Intel (Intel IoT Platform – платформа для IoT, лабораторія Інтернету речей Intel Ignition Lab), Microsoft (операційна система Windows 10 IoT, фреймворк AllJoyn, хмарний сервіс Azure), IBM (IBM Bluemix - понад 100 відкритих програмних інструментів і хмарних сервісів, IBM Cloud) та багато інших не менш відомих фірм.

Лише одна IBM інвестує в IoT 3 млрд. доларів, а кількість підключених до Інтернету пристроїв зросте в 2020 р. до 25 млрд. [2]. Тому не має сумнівів, що нова технологія IoT завоює світ.

Для реалізації функцій IoT необхідне наступне:

- спосіб, за допомогою якого пристрої будуть з’єднані між собою;
- шлях для збору даних з пристроїв;
- спосіб для обробки отриманих даних, щоб прийняти відповідні рішення.

З метою апробації нових навчальних курсів на базі мережевої Академії МікроТік, створеної в НТУУ «КПІ» в 2013 р., працюють гуртки (факультативи), які дозволяють за 5 навчальних семестрів додатково надати студентам необхідні знання для реалізації названих функцій IoT.

Заняття відрізняються практичною направленістю, а їх матеріали доступні на сайті Академії (mikrotik.kpi.ua) (рис. 3).

В 4-му навчальному семестрі вивчаються основи передачі даних від датчиків (SPI, I2C, OneWire, Bluetooth та ін.) з використанням Arduino. Накопичений досвід дозволяє стверджувати, що Arduino може вивчатися вже в 1 семестрі в курсі «Введення в спеціальність», коли студенти вже мають

перші навички програмування, а практичне їх застосування стає сильною мотивацією.

В 5-му семестрі студентам пропонується просунутий курс з використання мікрокомп'ютера Raspberry Pi [4], який Microsoft вибрав основним для впровадження своїх розробок IoT. Доступна вартість Raspberry Pi (в Україні близько 40$) дозволила створити 8 робочих місць для студентів.

В 6-му семестрі вже створюють проекти з використанням мови Python та Raspberry Pi. Практика після 3 курсу в Академії МікроТік дозволить студентам вивчити питання безпеки пристроїв IoT, налаштовуючи файрволи та VPN на маршрутизаторах МікроТік.

В 7-му семестрі розглядаються питання створення мобільних гаджетів, а побудові суцільної системи IoT присвячений 8-й семестр – для цього використовується власний сервісний сайт (iot.kpi.ua)

Також на РТФ в 2016-17 роках виконується ініціативна НДР «Радіотехнічні пристрої та системи для Інтернету речей», що дозволить студентам виконувати реальні курсові і дипломні роботи в галузі нових технологій.

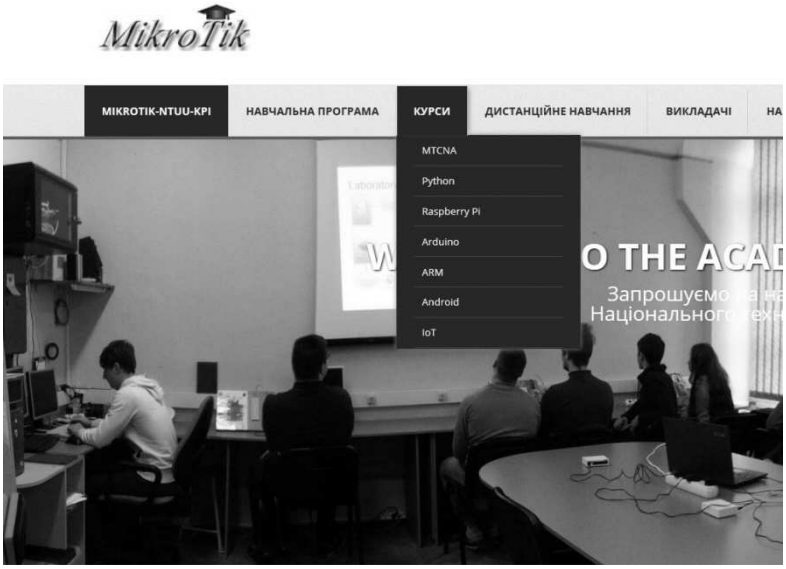


Рис. 3 Додаткові курси на РТФ для підготовки до впровадження технологій IoT.

Інтернет речей є новим етапом розвитку Інтернету, який значно розширює можливості збору, аналізу і розподілу даних, які людина може перетворити в інформацію та знання. В цьому сенсі Інтернет речей набуває величезного значення і підготовка спеціалістів актуальна в часі.

Література

1. Gartner's 2012 Hype Cycle for Emerging Technologies. Доступно на http://www.gartner.com/newsroom/id/2124315
2. Gartner's 2015 Hype Cycle for Emerging Technologies. Доступно на http://www.gartner.com/newsroom/id/3114217
3. *Найдич А*. «Интернет вещей» — реальность или перспектива? *КомпьютерПресс*, 2013, №12. Доступно на http://compress.ru/article.aspx?id=24290
4. *Могильний С.Б.* Мікрокомп'ютер Raspberry Pi – інструмент дослідника / С.Б. Могильний. - К.: Талком, 2014. — 340 с.

УДК 621.319

ЗАСІБ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ НАВЧАННЯ СПЕЦІАЛІСТІВ ПРАКТИЧНИМ НАВИЧКАМ ПРИ РОБОТІ З ТЕХНІЧНИМИ ПРИСТРОЯМИ

Рябенко М.С., Голь В.Д., Явіся В.С.
Державний заклад Інститут спеціального зв'язку та захисту інформації НТУУ «КПІ», Україна

Email: rmaxsept@gmail.com

Way to improving efficiency of training specialists practical skills with working on technical means

The problem to learning practical use of technical means new generation is very important. A small number of jobs leads to poor learning efficiency, which leads to a lack of highly qualified personnel. I propose a method to solve this problem by developing software that emulated the system in real time.

Однією з актуальних проблем в Україні є перехід від застарілих засобів телекомунікацій до більш нових. Перехід до використання нових технологій ускладнюється наявністю недостатньої кількості спеціалістів, які б могли експлуатувати та підтримувати в працездатному стані технічні пристрої нового зразку. Одним з прикладів цього є перехід до використання гнучких цифрових мультиплексорів взамін морально та технологічно застарілих що використовуються в наш час.

В умовах економічного, політичного та військового становища в України перехід до нових технологій є необхідним, включаючи використання військових засобів телекомунікацій застарілих зразків, якими володіють і інші держави. Навчання нових кадрів ускладнюється низькою проблем, таких як наявність матеріально-технічної бази та літератури.

Проблему нестачі матеріально-технічного забезпечення можна вирішити шляхом закупівлі потрібних зразків техніки та посібників, але це потребує значних економічних затрат. Як правило, якщо вартість літератури не є великою, то вартість технічних засобів може перевищувати сотні тисяч гривень, тому кількість навчальної техніки обмежена лише декількома зразками.

Достатня теоретична підготовка являється лише підґрунтям до застосування техніки в реальних умовах, тому здобуття практичних навичок являється обов'язковим. Мала кількість робочих місць для проведення практичних робіт не може забезпечувати достатній рівень підготовки молодих спеціалістів.

Для вирішення проблеми навчання на обмеженій кількості технічних засобів може вирішуватись декількома шляхами:

- Закупівля потрібної кількості техніки.
- Зменшення кількості навчаємих.

- Пошук альтернативних способів підготовки.

Перший спосіб являється досить ефективним проте не є можливим при обмеженому бюджеті.

Другий спосіб вирішує проблеми ефективного навчання, проте проблема збільшення кількості підготовлених спеціалістів лишається.

В наші часи в кожному вищому навчальному закладі експлуатуються комп'ютерні класи. Тому для вирішення проблеми швидкої підготовки чи перепідготовки спеціалістів пропоную розробити програмне забезпечення для тренування практичних навичок в роботі з необхідною технікою. Для створення програми необхідно врахувати декілька обмежень:

- Можливість встановлення програмного забезпечення на комп'ютери з слабкими характеристиками.
- Розроблення інтуїтивно зрозумілого інтерфейсу.
- Максимальна подібність програмного забезпечення до реальних зразків техніки.
- Можливість створення комплексів тренувальних програм з урахуванням реальної поведінки техніки в різних умовах.
- Документування програмного коду для подальшої її підтримки в актуальному стані.

Для розробки програмного забезпечення з урахуванням вище встановлених обмежень потрібно підібрати таку мову програмування, за допомогою якої можна не тільки створити програмний засіб але й в подальшому можливо було і підтримувати. Підтримка програмного забезпечення ґрунтується на модернізації технічних засобів з часом, тому програму слід оновлювати до актуального стану згідно з технічним зразком.

При виборі мови програмування потрібно також враховувати такі особливості як:

- Актуальність мови програмування та її підтримка з боку розробників.
- Складність написання коду.
- Наявність технологій до написання даної програми.

Мова програмування C# є відносно новою мовою програмування. Володіє всіма якостями перерахованими вище, має досить високі результати по швидкодії, не вимагає великої кількості ресурсів для своєї роботи та не тяжка у подальшій її підтримки у актуальному стані [1].

Розробка програми буде вестись в середовищі програмування Visual Studio. При розробці програмного забезпечення для створення інтерфейсу користувача буде використовуватись платформа .NET Framework з використанням Windows Forms [2][3].

Для створення максимально подібного інтерфейсу техніки буде використовуватись заздалегідь зібрана інформація, а саме фото реальних зразків техніки у всіх можливих її станах. Такий спосіб збору інформації досить тривалий, проте робота з програмою не буде відрізнятись від роботи на реальних зразках.

Процес створення програмного забезпечення складатиметься з декількох етапів: створення проекту, безпосередня розробка програми, створення документації та тестування.

Реалізована програма буде складатись з декількох частин, таких як:

- Інтерфейс користувача.
- Документація.
- Додаток для розробки практичних завдань.

Інтерфейс користувача представляє собою вибір практичного завдання та відображення зразків реальних технічних засобів. Інтерфейс має дві частини, в одній відображається хід виконання завдання з поясненнями та помилками, які виникли під час роботі з програмою, а саме з технічним засобом. В другій частині програми буде відображатись сама апаратура зв'язку, яка є повністю інтерактивною згідно до оригіналу.

Документація складається з декількох розділів які будуть містити різну інформацію. В першому розділі буде знаходитись інформація необхідна для роботи з програмою. В цьому розділі буде знаходитись пояснення результатів роботи програми при виконанні певної дії. В другому розділі буде знаходитись інформація яка необхідна для роботи з технікою зв'язку, а саме це буде документація по експлуатації технічних засобів.

Додаток для розробки практичних завдань потрібен для створення практичних програм для роботи з технікою. Цей додаток представлятиме собою окреме програмне забезпечення в якому можна буде створювати комплекси вправ та занять на роботі з технікою що дасть змогу створювати навчальні програми для роботи з технікою різної складності.

По закінченню виконання практичного плану програма видасть результат, який включає час виконання завдання та кількість помилок допущених при виконанні, що дасть змогу до аналізу своєї роботи.

Отже такий підхід до створення робочих місць для набуття практичних навичок у роботі з засобами телекомунікацій вирішує поставлене завдання. З економічної точки зору розробка програмного забезпечення не є багатовартісною. Кількість робочих місць, тобто навчаємих, обмежена лише кількістю персональних комп'ютерів, що є питанням, яке достатньо легко регулюється.

Література

1. Найгел К. C# 4 и платформа .NET 4.0 для профессионалов / Кристиан Нейгел, Билл Ивьен, Джей Глинн [та ін.] ; 2011 - 1435 с.
2. Ватсон К. Введение в C# / К. Ватсон ; 2004 - 879 с.
3. Рихтер Дж. CLR via C#. Программирование на платформе Microsoft .NET Framework 4.5 на языке C#. 4-е изд./ Дж. Рихтер; 2013 - 893 с.

УДК 621.382

МНОГОКРИТЕРИАЛЬНЫЙ ВЫБОР ОПТИМАЛЬНЫХ СРЕДСТВ ТЕЛЕКОММУНИКАЦИЙ

Безрук В.М., Чеботарёва Д.В., Скорик Ю.В.
Харьковский национальный университет радиоэлектроники
E-mail: valeriy_bezruk@ukr.net

Multicriterial choice of optimal telecommunications means

Theoretical and practical aspects of choosing the optimal version of telecommunications means taking into account the totality of quality indices are considered.

Интенсивное развитие отрасли телекоммуникаций, серьезная конкуренция заставляет операторов связи использовать оптимальные средства телекоммуникаций, которые используются при планировании и проектировании информационно-телекоммуникационных систем. При этом должна учитываться совокупность показателей качества, определяемых противоречивыми технико-экономическими требованиями к выбираемым проектным вариантам средств телекоммуникаций. Раньше при проектировании ограничивались только выбором допустимых вариантов средств телекоммуникаций с учетом заданных ограничений на показатели качества. При усложнении и увеличении стоимости информационно-телекоммуникационных систем актуальным является выбор оптимальных средств телекоммуникаций по заданному критерию оптимальности. Критерий оптимальности определяет предпотчтение одного проектного варианта перед другим с учетом совокупности противоречивых показателей качества, характеризующих средства телекоммуникаций. Это определяет необходимость применения многокритериального подхода не только к выбору оптимальных средств телекоммуникаций и построению на их основе информационно-телекоммуникационных систем, но и к организации бизнес-процессов в таких системах и обслуживанию пользователей с требуемым качеством обслуживания. Поэтому принятие оптимальных проектных решений с учетом совокупности показателей качества на основе методов многокритериальной оптимизации в настоящее время имеет особую важность для операторов связи.

Многокритериальный анализ и оптимизация достаточно широко развиты и используются в различных технических отраслях, однако они ещё недостаточно широко используются при планировании и проектировании информационно-телекоммуникационных систем. Одна из причин состоит в том, что проектировщики ещё не полностью осознали и используют широкие возможности математических методов многокритериальной оптимизации при решении практических задач выбора оптимальных средств телекоммуникаций с учетом совокупности показателей качества. В данной работе излагается методология многокритериального выбора оптимальных вариантов средств телекоммуникаций на базе основных положений теории многокритериальной

оптимизации, а также исследуются практические особенности ее применения на разных примерах из области телекоммуникаций.

Суть методологии многокритериального выбора оптимальных проектных вариантов. Важнейшим инструментом решения многокритериальных оптимизационных задач является принцип Эджворта–Парето (принцип Парето). При формулировке принципа Эджворта–Парето, постановку обычной многокритериальной задачи, включающей множество возможных решений и набор критериев (векторный критерий), дополняют бинарным отношением предпочтения лица, принимающего решения (ЛПР). Принцип Эджворта–Парето формулируется в виде утверждения о том, что выбираемые решения содержатся только в множестве Парето. Применение принципа Эджворта–Парето позволяет из множества всех возможных вариантов исключить заведомо неприемлемые решения - те, которые никогда не могут оказаться выбранными (если выбор осуществляется достаточно «разумно»). После такого исключения остается множество, которое называют множеством Парето или областью компромиссов. Иначе говоря, каждое выбираемое решение является Парето–оптимальным. Полученное множество Парето, как правило, является достаточно широким и при окончательном выборе решений неизбежно возникает вопрос о том, какое именно единственное решение выбрать среди Парето–оптимальных.

Когда возникает необходимость сужения подмножества Парето, то единственный предпочтительный проектный вариант может выбираться с привлечением дополнительной субьективной информации от экспертов, отражающей предпочтения ЛПР. Такая информация появляется в результате всестороннего анализа Парето-оптимальных решений, многомерных рабочих характеристик, многомерных диаграмм обмена, относительной важности введенных целевых функций и др. Полученные при этом дополнительная информация о предпочтениях используются для построения некоторого условного критерия предпочтения, основанного, в частности, на введении некоторой скалярной функции, оптимизация которой приводит к выбору единственного варианта системы. Рассматриваются различные формализованные методы сужения подмножества Парето–оптимальных решений до единственного предпочтительного варианта с учетом субьективной информации от экспертов, в частности, основанные на теории полезности, теории нечетких множеств, лексографических отношениях, анализе иерархий.

Практические особенности применения методов многокритериальной оптимизации при выборе оптимальных проектных вариантов средств телекоммуникаций (СТ) с учетом формализованного учета совокупности показателей качества включает в себя следующие этапы:

- задание набора исходных данных для допустимых проектных вариантов СТ; - определение множества допустимых проектных вариантов с учетом ограничений на структуру и параметры СТ; - задание показателей показателей качества СТ и вычисление их значений для допустимых проектных вариантов; - выбор подмножества Парето-оптимальных проектных вариантов СТ в критериальном пространстве оценок значений показателей качества; - анализ полученых Парето-оптимальных проектных вариантов, многомерных потенциальных характеристик и многомерных диаграм обмена показателей

качества СТ; - формирование условного критерия предпотчтения с привлечением полученной дополнительной информации от экспертов для выбора единственного проектного варианта СТ.

В работе рассматриваются разные методы нахождения множества Парето-оптимальных проектных решений. В частности, метод дискретного выбора состоит в том, что включение проектного решения в множество Парето имеет место тогда и только тогда, когда не существует других предпочтительных решений. Рассматриваются также специальные методы нахождения Парето-оптимальных решений. Метод рабочих характеристик сводится к нахождению экстремума одной из частных целевых функций при условии, что на остальные целевые функции накладываются ограничения типа равенства. Решение множества таких скалярных оптимизационных задач с разными допустимыми вариантами ограничений приводит к Парето-оптимальным решениям. Весовой метод состоит в нахождении экстремумов взвешенной суммы частных целевых функций при разных комбинациях весовых коэффициентов. Применение этого метода также дает множество Парето-оптимальных решений. Рассматриваются и другие методы нахождения Парето-оптимальных решений, в частности, метод главного критерия, метод последовательных уступок. Формализованное решение задач многокритериальной оптимизации сводится лишь к нахождению некоторого множества Парето–оптимальных решений и исключению безусловно худших решений. Все Парето–оптимальные решения являются несравнимыми между собой и каждое из них может быть использовано для последующих этапов проектирования.

Предложенная методология многокритериального выбора оптимальных проектных решений использована для выбора оптимальных проектных вариантов средств телекоммуникаций с учетом совокупности противоречивых показателей качества. В частности, исследованы особенности ее применения для различных типов средств телекоммуникаций, в частности, речевых кодеков, модемов в системе цифровой связи, технологий цифрового телевидения, технологий в сетях мобильной связи второго, третьего и четвертого поколений, систем массового обслуживания заявок и вариантов построения в сетях передачи данных, маршрутизации и алгоритмов управления в сетях связи. В каждой из задач из заданного допустимого множества вариантов средств телекоммуникаций одним из рассмотренных методов найдено подмножество Парето-оптимальных вариантов и выделен единственный предпочтительный вариант средств телекоммуникаций.

Литература

1. *Чеботарёва Д.В., Безрук В.М.*. Многокритериальная оптимизация проектных решений при планировании сотовых сетей мобильной связи. - Харьков: СМИТ, 2013. - 148 с.
2. *Bezruk V.M., Skorik Yu.V.* Multicriterial choice of telecommunications means using hierarchical analysis method // Information and Telecommunication Sciences. – K: NTU “KPI”, 2015. - Vol. 6, Num. 2. - P. 18-24.

УДК 621.391

МОДЕЛЬ ВІРТУАЛЬНОГО МАРШРУТИЗАТОРА З СТАТИЧНОЮ ТА ДИНАМІЧНОЮ РЕКОНФІГУРАЦІЄЮ РЕСУРСІВ

Червенець В.В., Бешлей М.І., Романчук В.І. Поліщук А.В.
Інститут телекомунікацій, радіоелектроніки та електронної техніки
Національний університет «Львівська політехніка», Україна
E-mail: beshlebmi@gmail.com, v.chervenets@polynet.lviv.ua, romanchuk@lp.edu.ua

Model of virtual router with static and dynamic resource reconfiguration

This paper looks into a novel network router architecture, which could improve the Quality of Service guarantees which can be provided to such flows. This router architecture makes use of virtual machine techniques, to assign an individual virtual router to each network flow requiring QoS guarantees.

На сучасному етапі розвитку інформаційних та телекомунікаційних технологій, коли мультисервісні мережі використовують стандартну мережеву інфраструктуру з пакетною передачею даних, для надання всієї гами існуючих послуг, які є симбіозом передачі даних, голосу і відео, мережі все частіше стають вузьким місцем при передаванні трафіку з використанням існуючих протоколів та методів. Тому науковці працюють в напрямку дослідження і підвищення якості надання послуг [1]. Експоненційне збільшення розміру трафіку при відставанні базової місткості мереж, тобто інтенсивного збільшення мережевих ресурсів (буферного простору в вузлах комутації, пропускної здатності каналів передавання, розрахункових потужностей, часу прийняття керуючих дій), змушує шукати ефективні механізми забезпечення якості обслуговування як комплексного програмно-апаратного рішення в маршрутизаторах та комутаторах.

Дану задачу пропонується вирішити шляхом використання методів віртуалізації ресурсів для розгортання в одному фізичному маршрутизаторі декількох віртуальних, призначених для індивідуальної обробки послуг одного класу із своїми вимогами до QoS. Для підтвердження або спрощення гіпотези віртуалізації мережевого пристрою з метою забезпечення гарантованого рівня QoS в роботі необхідно порівняти існуючі технічні рішення при використанні стандартного маршрутизатора та розробленим у роботі прототипу експериментального маршрутизатора, який використовує технологію віртуалізації ресурсів. Перш ніж приступити до створення маршрутизатора з віртуалізацією ресурсів потрібно зрозуміти основні поняття та принципи функціонування існуючих стандартних маршрутизаторів. Найчастіше в комутаторах та маршрутизаторах застосовуються такі механізми обробки черг за принципом FIFO та пріоритетного обслуговування, проте навіть при їх використанні немає строгих гарантій забезпечення збалансованого завантаження мережевих ресурсів та необхідного рівня обслуговування різнорідних трафіків користувачів у мультисервісних ТКС.

В роботі запропоновано новий підхід до побудови мультисервісної інфраструктури з віртуалізацією маршрутизаторів. Мультисервісна мережа з віртуалізацією – це мережа в якій на одному або декількох мережевих пристроях використовується режим роботи з віртуалізацією. Віртуалізація мережевого пристрою передбачає створення двох або більше віртуальних мережевих машин, які виконують функції маршрутизатора з індивідуальним обслуговуванням потоків. В даному випадку для простоти формалізації моделі віртуального маршрутизатора розглядається передавання трьох типів сервісів так званих послуг Triple play (голос, відео і дані). Відповідно при розроблені структури мережевого пристрою з віртуалізацією, розгорнуто три віртуальні маршрутизатори. Призначені для індивідуального обслуговування потоків одного типу, забезпечуючи їм необхідний рівень QoS згідно вимог, шляхом виділення фізичних ресурсів апаратного мережевого пристрою для конфігурації необхідних продуктивностей віртуальних маршрутизаторів обробки інформаційних потоків (голосу, відео та даних). Розглянемо принцип роботи запропонованого маршрутизатора з віртуалізацією ресурсів.

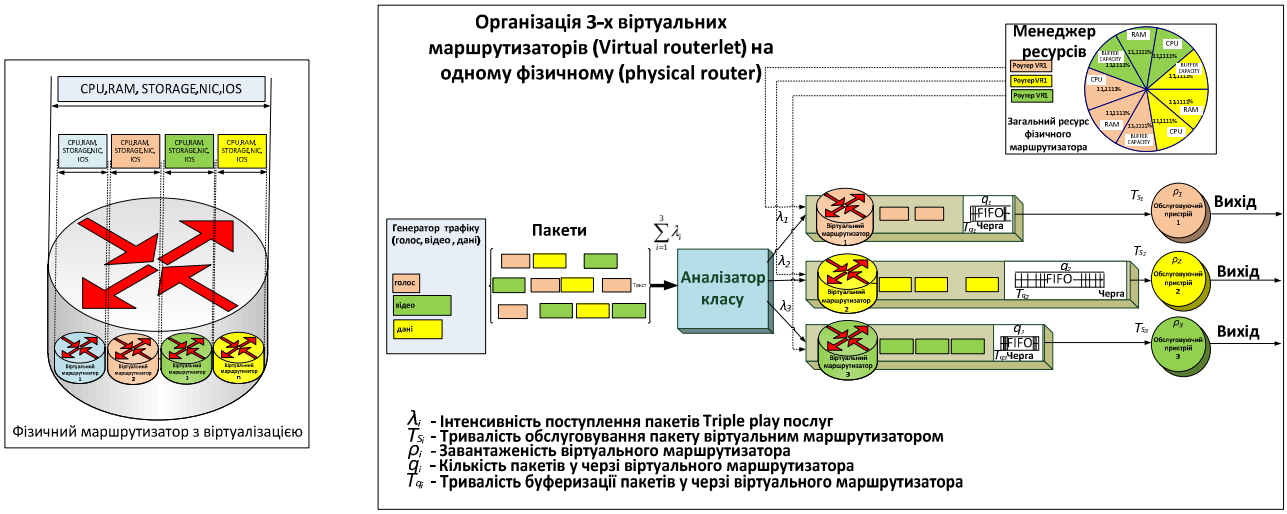


Рис.1.Модель пакетного маршрутизатора з статичною та динамічною віртуалізацією ресурсів.

На вхід віртуального маршрутизатора (рис.1) поступає агрегований потік пакетів з інтенсивністю $\Delta = \sum_{i=1}^{n} \lambda_i$. Сумарний потік у цьому разі складається з n частинних потоків, де n=3 (голос,відео і дані), кожний з яких характеризується власними параметрами і розподілом. Після чого вхідний потік пакетів з сумарною інтенсивністю, поступає на мережевий пристрій обробляться і розділяться на N=3 мережевих віртуальних пристроїв згідно пріоритету поля сервісу Type of Service (ToS), DSCP. Розділення на віртуальні пристрої відбувається блоком аналізатор класу, який працює на основі аналізу IP заголовка і в залежності від вмісту DSCP чи ToS поля зчитуватиме код, який вказуватиме на відповідний тип сервісу та направлятиме їх на обслуговування віртуальними маршрутизаторами класового призначення. Даний принцип розподілу на маршрутизатори є

подібним механізму розподілу пакетів на черги різної пріоритетності системи пріоритетного обслуговування. Тому, технічно при віртуалізації мережевого пристрою, функції блоку класифікації залишаються без змін, направлений лише під інакшу задачу. Відповідно при порівнянні тривалостей затримки віртуального маршрутизатора із існуючим маршрутизатором за принципом пріоритетного обслуговування, час обробки поля пріоритету сервісу є однаковим та сталим для віх послуг і є значно менше часу обробки заявки в маршрутизаторі. Таким чином даним часом можна знехтувати. Головним чинником по ступеню впливу на виникнення черг, які призводять до важкопрогнозованих затримок буферизації пакетів є коефіцієнт завантаження віртуального пристрою – відношення середньої інтенсивності вхідного потоку λ_i до середньої інтенсивності передавання пакетів на вихідний інтерфейс μ_i .(в моделі під даним параметром розуміється T_{Si} - тривалість обслуговування пакету *i*-го потоку віртуальним маршрутизатором. Перевагою даної моделі є те, що при використанні блоку менеджера управління ресурсів, який функціонально відповідає гіпервізору при організації віртуальних машин є можливість статично та динамічно виділяти обчислювальні ресурси мережевого пристрою для віртуальних маршрутизаторів в залежності від вимог QoS потоку. Під обчислювальними ресурсами пристрою будемо розуміти апаратні ресурси, конфігурація яких суттєво впливає на можливість і продуктивність виконання обробки пакетів віртуальним вузлом. В свою чергу, апаратна конфігурація кожного вузла це об’єм його оперативної пам’яті, тактової частоти процесора та буферної пам’яті. Які виділяються статично та динамічно в залежності від прогнозування вхідного навантаження потоків на вузол, виділяючи необхідні ресурси віртуальним маршрутизаторам реконфігуруючи їх продуктивності в певні моменти часу. Такий підхід дасть змогу динамічно створювати ефективні віртуальні СМО з оптимальними параметрами (довжина черги, дисципліна керування переповненням черги, кількість обслуговуючих пристроїв, режим роботи обслуговуючих пристроїв) для певного типу сервісів з набором властивих їм вимого до параметрів мережі(втрати, затримки та джитер).

Висновки. Розроблено модель віртуального маршрутизатора, використання яких в мультисервісній інфраструктурі забезпечить ефективний розподіл між різними мережевими потоками та дасть змогу підвищити якість обслуговування потоків реального часу із наданням гарантованого рівня QoS сервісів чутливих до втрат та нечутливих до затримок.

Література

1. Beshley M.M. Increasing the efficiency of real-time content delivery by improving the technology of priority assignment and processing of IP traffic / M. Beshley, M. Seliuchenko, O. Lavriv, V. Chervenets, H. Kholiavka, M. Klymash // Smart Computing Review, - 2015.- Vol.5,- No.2. – P.76-88

УДК 519.8

ДО ВИМІРЮВАННЯ СИСТЕМНИХ РИЗИКІВ МЕРЕЖ

Горбачук В.М., Морозов О.О.
Інститут кібернетики імені В.М.Глушкова НАН України, Україна
E-mail: GorbachukVasyl@netscape.net

Розглядаються мережі як складні системи (від транспортних і логістичних мереж у формі ланцюгів постачання до фінансових мереж та Інтернет). Розробляються концепції, визначення, структури математично строгих і комп'ютеризованих засобів оцінювання роботи й ефективності мереж. Пропонуються методи аналізу робастності та вразливості.

To measuring network systemic risks

Networks are considered as complex systems (from transportation and logistics networks in a supply chain form to financial networks and Internet). The concepts, definitions, structures of mathematically strict and computerized tools for network performance and efficiency estimation are developed. The techniques of robustness and vulnerability analysis are suggested.

Нові теорії безмасштабних мереж малого світу значно поліпшили розуміння поведінки і вразливості багатьох мереж реального світу [1–3]. Однак більшість досліджень вразливості мереж зосереджувалася на таких топологічних характеристиках мереж, як зв'язність або довжина найкоротшого шляху мережі [4]. Хоча топологічна структура мережі дає критичну інформацію стосовно вразливості мережі, потік по мережі є таким же важливим індикатором, як економічні показники (індуковані потоком витрати, зміна поведінки користувачів після розривів тощо): «щоб досягти розуміння складності, слід вийти за межі структури і топології та починати зосереджуватися на динаміці, яка має місце вздовж зв'язків; мережі є лише каркасом складності, великими дорогами для різних процесів, які оживляють наш світ» [5].

Запропонована міра ефективності мережі, яка має переваги порівняно з кількома іншими існуючими мірами [6–9]. Ця міра була застосована до вивчення мережі метро м. Бостон (MBTA) та Інтернет. Оскільки ця міра розглядає лише геодезичну інформацію, то не охоплює такі важливі фактори, як потоки мережі, пов'язані витрати, поведінку користувачів за принципів централізованого чи децентралізованого прийняття рішень.

Тому потрібні теоретичні і практичні основи нової міри результативності чи ефективності мережі, що узагальнюють міри [6–9] та враховують такі суттєві характеристики мережі, як потоки, індуковані прийняттям рішень, і вартості оцінювання важливості компонентів мережі серед розмаїття мережевих систем. Можна запропонувати нову міру ефективності мережі, що має значні переваги порівняно з рядом існуючих мір і враховує особливості мереж реального світу, явно розглядаючи перенавантаження. Більше того, ця міра може застосовуватися до мережевих задач як з фіксованим, так і з еластичним попитом, а також до залежних у часі динамічних мереж (якими є Інтернет, мережі генерації і розподілу електроенергії). Ця міра дозволяє ранжувати

компоненти мережі (вузли і ланки) чи їхні комбінації у термінах їхньої важливості з погляду економічних результатів. Ця міра корисна не лише для планування й експлуатації, але й для національної безпеки.

Крім того, замість обчислення й оцінювання впливу від повного розриву чи видалення компоненту мережі формалізуємо інший важливий аспект, пов'язаний з вразливістю мережі, – поняття робастності мережі. Робастність мережі стосується зменшення таких мережевих ресурсів, як місткість ланки. Інститут інженерів електрики й електроніки (Institute of Electrical and Electronics Engineers, IEEE) у 1990р. визначає робастність як «ступінь, до якого система чи компонент може правильно функціонувати у присутності невірних входів або стресових умов» [10]. Тема робастності особливо доречна і своєчасна для США через постійні повідомлення про те, що колись краща у світі інфраструктура США зазнає помітного старіння й занепаду, збільшуючи вразливість мереж і населення. Наприклад, понад чверть 590750 мостів США оцінюються як структурно недосконалі чи функціонально застарілі. Деградація транспортних мереж внаслідок поганої експлуатації, природних лих, старіння, непередбачуваних нападів на початку 21-го сторіччя завдавала збитків США на 94 млрд.дол. лише у частині потреби ремонту доріг. Погані умови доріг США коштують автомобілістам 54 млрд.дол. щороку на ремонт і експлутаційні витрати. З іншого боку, за 1960–2004 рр. у США число автомобілістів зросло на 157 млн. (або на понад 212%), а кількість ліцензованих водіїв зросла на 109 млн. (або на понад 125%) [11], збільшуючи тиск на вже крихкі транспортні мережі США. Внаслідок розладів транспортних мереж США і зростаючої кількості транспортних засобів пасажири США щороку витрачають 3.5 млрд.год. на стояння у трафіку, що еквівалентно втратам 63.2 млрд.дол. для економіки [12]. Водночас США зазнає кризи вантажної місткості, яка загрожує потужності і продуктивності всієї економіки [13]. За даними Асоціації дорожних і транспортних будівельників США, близько 70% вантажів перевозиться на швидкісних дорогах, де корки щороку спричинюють затримки дальнобійників на 243 млн.год., еквівалентні втратам 8 млрд.дол. для економіки [14]. Уряд США зіштовхнувся з дефіцитом 1.6 трлн.дол. на ремонт і реконструкцію інфраструктури у 2008–2012 рр. [15].

Таким чином, побудова прийнятних мір робастності мереж має теоретичне і практичне значення. Для різної поведінки користувачів можна будувати такі міри, придатні для аналізу транспортних мереж. Це особливо важливо через парадокс Браесса [16], де додання нової дороги при поведінці користувачів, кожний з яких оптимізує свою ціль, може збільшити час або витрати для всіх. Крім того, слід вводити індикатори оцінки впливу на довкілля, щоб моделювати залежність навколишнього середовища від деградації мереж. Також варто кодифікувати міри впливу інвестицій у мережеву інфраструктуру на поліпшення місткості (пропускної здатності).

Сучасні суспільство й економіка залежать від такої критичної інфраструктури, як транспортні, логістичні і комунікаційні мережі, включаючи Інтернет, мережі генерації і розподілу електроенергії, фінансові мережі. Отже, точні засоби ідентифікації вузлів і ланок, що справді є важливими у таких мережевих системах і тому мають краще утримуватися, дають суттєву

інформацію для осіб, які приймають рішення, – від урядових працівників і розробників політики до плановиків, інженерів, учених, керівників організацій і корпорацій [17]. Уніфікована міра ефективності мережі за децентралізованої поведінки користувачів, кожний з яких оптимізує свою ціль, основана на фундаментальних методологіях, мережевих моделях різної поведінки прийняття рішень, засобах кількісного аналізу, алгоритмах пошуку розв'язків мережевих задач.

Література

1. *Amaral L.A.N., Scala A., Barthelemy M., Stanley H.E.* Classes of small-world networks // Proceedings of the National Academy of Sciences USA. – 2000. – 97. – P. 11149–11152.
2. *Chassin D.P., Posse C.* Evaluating North American electric grid reliability using the Barabasi–Albert network model // Physica A. – 2005. – 355. – P. 667–677.
3. *Holmgren A.J.* A framework for vulnerability assessment of electric power systems / Reliability and vulnerability in critical infrastructure: a quantitative geographic perspective. A. Murray, T. Grubesic (eds.) – New York: Springer, 2007. – P. 31–55.
4. *Callaway D.S., Newman M.E.J., Strogatz S.H., Watts D.J.* Network robustness and fragility: percolation on random graphs // Physical review letters. – 2000. – 85. – P. 5468–5471.
5. *Barabasi A.L.* Linked: how everything is connected to everything else and what it means. – New York: Plume, 2003.
6. *Latora V., Marchiori M.* Efficient behavior of small-world networks // Physical review letters. – 2001. – 87. – 198701.
7. *Latora V., Marchiori M.* Is the Boston subway a small-world network? // Physica A. – 2002. – 314. – P. 109 –113.
8. *Latora V., Marchiori M.* Economic small-world behavior in weighted networks // The European physical journal B. – 2003. – 32. – P. 249–263.
9. *Latora V., Marchiori M.* How the science of complex networks can help developing strategies against terrorism // Chaos, solitons and fractals. – 2004. – 20. – P. 69–75.
10. IEEE standard computer dictionary: a compilation of IEEE standard computer glossaries. – New York: Institute of Electrical and Electronics Engineers (IEEE), 1990.
11. Highway statistics 2004. – Washington, DC: Federal Highway Administration; U.S. Department of Transportation. – http://www.fhwa.dot.gov
12. Report card for America's infrastructure. – American Society of Civil Engineers, 2005. – http://www.asce.org/reportcard/2005/index.cfm
13. An initial assessment of freight bottlenecks on highways. – Washington, DC: U.S. Department of Transportation Federal Highway Administration, 2006. – http://www.fhwa.dot.gov/policy/otps/bottleneck/
14. *Jeannert M.* Federal government freight bottleneck report highlights America's growing transportation infrastructure crisis. – Road & Transportation Builders Association, 2006. – http://www.artba.net/news/press_releases/2006/02-03-06.htm
15. Governors, mayor form coalition to rebuild ailing U.S. infrastructure // Environment News Service. – 2008, January 22. – http://www.ens-newswire.com/ens/jan2OO8/2008-01-22-02.asp
16. *Braess D.* Uber ein paradoxon aus der verkehrsplanung // Unternehmensforschung. – 1968. – 12. – P. 258–268.
17. *Горбачук В.М.* Методи індустріальної організації. Кейси та вправи. Економіка та організація виробництва. Економічна кібернетика. Економіка підприємства. – К.: А.С.К., 2010. – 224 с.

УДК 621.391:006

ОЦЕНКА СТАБИЛЬНОСТИ СИГНАЛОВ СИНХРОНИЗАЦИИ В СОВРЕМЕННЫХ ПАКЕТНЫХ СЕТЯХ

Бирюков Н.Л., Триска Н.Р., *ИТС НТУУ "КПИ", Украина*
E-mail: nlbir@mail.ru
Худынцев Н.Н., *ОГЭКУ, Украина*

Evaluation of timing stability in up-to-date packet networks

Some metrics proposed for timing stability evaluation in packet networks are analyzed. The MTIE metrics family and metrics defined in ITU-T Recommendation G.8260 (notably MATIE, MAFE, *min*MATIE, and *min*MAFE) are compared. The suitability of these metrics for packet selection is discussed.

Фундаментальные изменения сетевой инфраструктуры, обусловленные повсеместным переходом к пакетным технологиям передачи и коммутации, не могли не повлиять на подходы к решению задач частотно-временного обеспечения. Базовыми методами синхронизации в современных пакетных сетях стали технология синхронного Ethernet (SyncE) и протокол точного времени PTP (IEEE1588v2). Все большую популярность приобретает комбинированный сценарий, предусматривающий совместное использование синхронного Ethernet для передачи тактовой частоты и протокола PTP для передачи точного времени [1]. При внедрении новых методов частотной и временной синхронизации и адаптации существующих методов к новым условиям возник целый ряд задач, требующих серьезной научной и практической проработки. Одна из таких задач – это подбор подходящих метрик, которые позволили бы наиболее эффективно оценить стабильность сигналов синхронизации в современном оборудовании пакетных сетей.

Следует отметить две тенденции в разработке метрик, способных учитывать особенности пакетного режима передачи с точки зрения обеспечения заданной точности частоты и фазы. Одна тенденция выражается в использовании традиционных метрик оценки качества сигналов синхронизации, например, максимального отклонения временного интервала – МОВИ (MTIE – Maximum Time Interval Error) и девиации временного интервала ДВИ (TDEV – Time Deviation) с расширением их возможностей [2] и/или адаптацией к условиям работы пакетных сетей [3].

Другая тенденция заключается в увеличении количества метрик, которые в той или иной степени отражают особенности пакетной передачи с точки зрения синхронизации по частоте или фазе. Например, последнее издание терминов и определений, относящихся к синхронизации пакетных сетей [4], включает дополнительные определения и оценочные формулы minTDEV и percentile TDEV (процентиль TDEV). Появились также новые усредняющие метрики, подобные TDEV, которые описывают максимальные фазовые или частотные девиации: MATIE (maximum average time interval

error) – максимальная средняя ошибка временного интервала ОВИ (МСОВИ); MAFE (maximum average frequency error) – максимальная средняя ошибка частоты МСОЧ; minMATIE и minMAFE. Целесообразность и эффективность использования предложенных функций подлежит дальнейшему изучению.

В [5, 6] исследовались общие свойства функции МОВИ и, на их основе, некоторые свойства ансамблей МОВИ, а также их связь с другими метриками, в частности, автокорреляционными функциями. Кроме того, предложено семейство функций от размахов ОВИ, а именно минимальное min[PtP(τ)] и среднее mid[PtP(τ)] отклонения размахов PtP(τ) на интервалах наблюдения τ. Функции min[PtP(τ)] и mid[PtP(τ)] обладают теми же свойствами, что и функция МОВИ($n\tau_0$) – неотрицательная, монотонная, неубывающая, вогнутая (выпукла вверх). Также эти функции отображают линейное смещение частоты и дрейф. В [6] показано, что на любом интервале наблюдения для данной выборки объемом N верно неравенство:

$$\min[\mathrm{PtP}(\tau)] \le \mathrm{mid}[\mathrm{PtP}(\tau)] \le \max[\mathrm{PtP}(\tau)] \equiv \mathrm{МОВИ}(\tau), \qquad (1)$$

откуда следует, что оценивание последовательности ОВИ по, например, min[PtP(τ)], дает лучшие результаты для подстройки часов по относительной разнице фаз тактовых частот передающих и приемных часов, чем традиционная функция ОВИ.

С точки зрения оценки качества сигналов и/или оценки соответствия передающих трактов в пакетных сетях, на практике требуется достаточно ограниченный набор метрик, который близок первой тенденции, с добавлением дисперсии задержки пакетов – PDV (packet delay variation) из второго направления. Соответствующие нормы уже появляются в нормативных документах (например, в [3]). Однако методики измерения PDV еще недостаточно отработаны. В частности, это касается способов выбора и фильтрации пакетов для оценки PDV.

Существующая неопределенность в части методик выбора и фильтрации последовательностей данных, получаемых из последовательностей поступления пакетов для оценки различных метрик, может повлиять на корректность полученных результатов. Вопрос отработки и стандартизации методик измерения параметров точности и стабильности в пакетных сетях еще находится в стадии изучения, и на данном этапе важно, чтобы предлагаемые решения прошли апробацию на сетях в условиях практической эксплуатации оборудования. Нормированные параметры и методики их измерения, с одной стороны, должны обеспечивать проведение корректных измерений с однозначными и достоверными результатами и, с другой стороны, должны быть удобными для практического применения в условиях эксплуатации.

Настоящая работа представляет результаты анализа различных последовательностей данных, который проводился аналитическими методами, с помощью моделирования, подобно [5,6], а также с использованием данных реальных измерений на сетях связи. Результаты в отношении расширенного семейства метрик МОВИ(τ), предложенного в [6],

оценок частоты по этим метрикам (FMpp(τ), Fstd(τ)), а также метрик [4] – MATIE(τ), MAFE(τ) и TDEVpkt(τ), представлены на рис. 1.

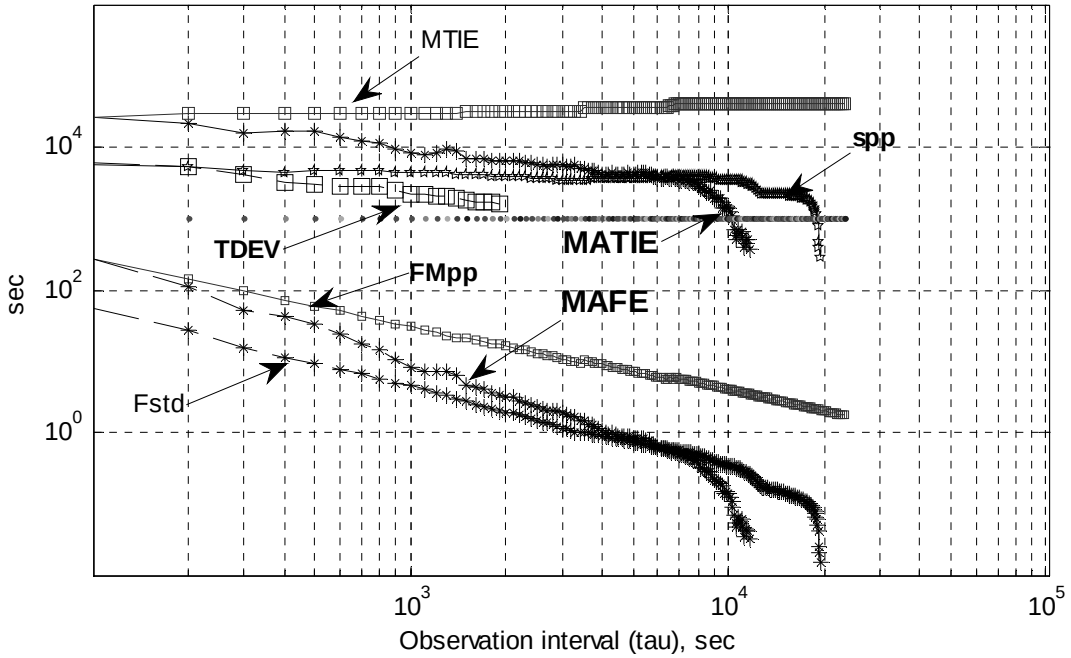


Рис. 1 Обработка данных серии измерений: МОВИ(τ) ≡ MTIE, MATIE, TDEV, MAFE.

Проведенный анализ показывает высокий уровень взаимной корреляции (ВФК) между различными метриками. Например, на равных интервалах наблюдения величина ВФК между МОВИ(τ) и MATIE(τ) составляет более 0,8, между FMpp(τ) и MATIE – не менее 0,95, а у FMpp(τ) и MAFE – 0,9. Данные иллюстрируют (1): МОВИ на интервалах наблюдения дает оценку сверху как по ОВИ, так и по частоте (FMpp). На основе полученных результатов можно предположить, что расширенные метрики на базе хорошо отработанной и надежно апробированной функции МОВИ позволяют получить сведения, которые перекрывают MATIE и MAFE.

Литература

1. Бирюков Н.Л., Триска Н.Р., Худынцев Н.Н. Обзор направлений исследований МСЭ в области частотно-временного обеспечения современных сетей связи. – T-Comm, № 2-2014. – с.12-17.
2. Бирюков Н.Л., Касим А.М., Триска Н.Р. Метрики оценки статистик стабильности сетей тактовой синхронизации с пакетной передачей сообщений. – Дев'ята Міжнародна науково-технічна конференція "Проблеми телекомунікацій" (ПТ-2015), 21-24 квітня 2015 р. Матеріали конференції. – с.122-124.
3. ITU-T Recommendation G.8261.1/Y.1361.1 (02/2012) Packet delay variation network limits applicable to packet-based methods (Frequency synchronization).
4. ITU-T Recommendation G.8260 (08/2015) Definitions and terminology for synchronization in packet networks.
5. Бирюков Н.Л., Триска Н.Р. Использование функции максимальной ошибки временного интервала для оценки состояния цифровых трактов. – "Зв'язок"-2004, № 1 – С. 50-54.
6. Бірюков М.Л. Оцінювання якості двохстороннього обміну повідомленнями точного часу за функціями відхилу часового інтервалу. – Збірник наукових праць ВІТІ НТУУ "КПІ" 2011, № 1. – С. 24-29.

УДК 621.319

ПОРІВНЯЛЬНИЙ АНАЛІЗ АСИМЕТРИЧНИХ КРИПТОГРАФІЧНИХ МЕТОДІВ

Толстова А.В., Голь В.Д., Правило В.В.
Державний заклад Інститут спеціального зв'язку та захисту інформації НТУУ «КПІ», Україна
E-mail: tolstova369@gmail.com

Comparative analysis of cryptographical systems

Comparative analysis of asymmetric cryptographic systems was made. The work algorithms of basic asymmetric cryptographic systems and results of them comparative analysis are presented.

В телекомунікаційних системах розрізняють шифрування повідомлень двох типів: симетричне (із секретним ключем) та асиметричне (з відкритим ключем) [1].

При *симетричному* шифруванні (рис. 1) створюється ключ, файл разом з ключем пропускається через програму шифрування та отриманий результат пересилається адресатові. Ключ передається адресатові окремо, використовуючи інший (захищений) канал зв'язку. Адресат, запустивши ту ж саму шифрувальну програму з отриманим ключем, зможе прочитати повідомлення.

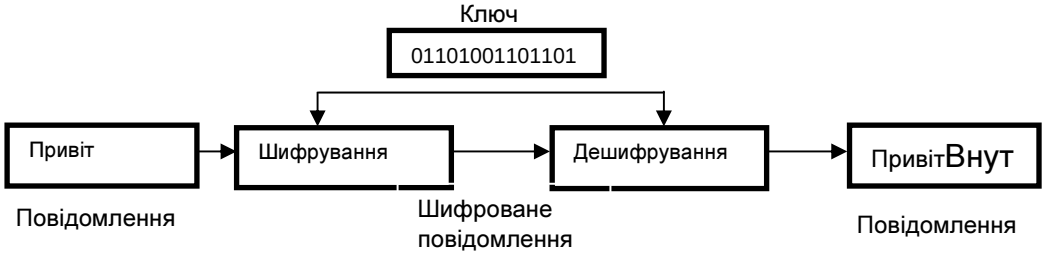


Рис. 1 Симетричне шифрування.

У *асиметричних* криптоалгоритмах (RSA, ElGamal, Diffie-Hellman) (рис. 2) пряме і зворотне перетворення виконуються з використанням відкритого і секретного ключів, що не мають взаємозв'язку, що дозволяє по одному ключу обчислити інший. За допомогою відкритого ключа практично будь-який користувач може зашифрувати своє повідомлення або перевірити електронно-цифровий підпис. Розшифрувати таке повідомлення або поставити підпис може тільки власник секретного ключа. Такі алгоритми дозволяють реалізувати протоколи типу цифрового підпису, забезпечують відкрите поширення ключів і надійну автентифікацію в мережі, стійку навіть до повного перехоплення трафіка [2].

Стійкість ***алгоритму RSA*** базується на складності факторизації великих цілих чисел. Відкритий і закритий ключі є функціями двох великих простих чисел розрядністю 100…200 десяткових цифр і навіть більше. Відновлення відкритого тексту за шифротекстом та відкритим ключем є рівнозначне до розкладання числа на два великі прості множники. Криптоаналіз ані доводить, ані спростовує безпеку алгоритму RSA, тим самим обґрунтовуючи міру довіри

щодо алгоритму.

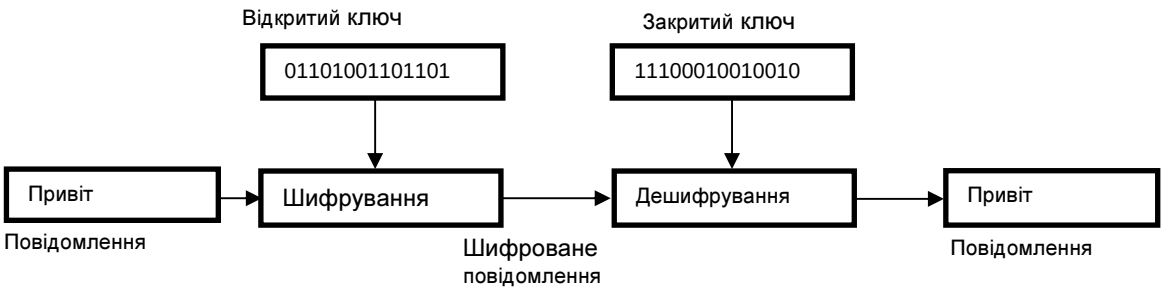


Рис. 2 Несиметричне шифрування.

У довільний спосіб обираються два великі прості числа p та q. Обчислюється добуток $n = pq$. Обчислюється функція Ейлера: $\varphi(n) = (p-1)(q-1)$.

Довільно обирається просте число e – ключ зашифровування, яке задовольняє умовам

$$e < \varphi(n);\ \text{НСД}(e, \varphi(n)) = 1.$$

Обчислюється число d – ключ розшифровування, яке є оберненим до числа e, тобто

$$ed \equiv 1 \pmod{\varphi(n)}.$$

Пара чисел (e, n) є відкритим ключем і розміщується у загальнодоступному довіднику, а числа p, q тримаються у секреті, d – секретний ключ. При шифруванні повідомлення M спочатку розкладається на цифрові блоки, розміри яких менше за n, тобто якщо p та q є 100-розрядними простими числами, то n міститиме близько 200 розрядів і кожен блок повідомлення m_i повинен мати близько 200 розрядів у довжину. Зашифроване повідомлення C складатиметься з блоків c_i такої самої довжини. Формула зашифровування буде мати вигляд:

$$C \equiv M^e \pmod{n}.$$

Розшифровування забезпечується операцією піднесення до степеня d за модулем n одержаного шифртексту C:

$$M \equiv C^d \pmod{n}.$$

Алгоритм Ель-Гамаля є альтернативою алгоритму RSA і при рівному значенні ключа забезпечує таку саму криптостійкість. Безпека алгоритму Ель-Гамаля базується на складності обчислювання дискретних логарифмів. Учасники інформаційного процесу обирають просте число p і ціле число q, який є первинним коренем за модулем p.

Сторона A генерує секретний ключ $k_a < p$ і обчислює відкритий ключ

$$Y_a \equiv q^{k_a} \pmod{p}.$$

Сторона B обирає число $k_b < p$ і за його допомогою зашифровує передаване повідомлення M у такий спосіб:

$$Y_b \equiv q^{k_b} \pmod{p} \quad \text{і} \quad C = M \oplus (Y_a^{k_b} \pmod{p}).$$

Величина M є послідовністю двійкових символів, які передаються до каналу зв'язку. Величина $Y_a^{k_b} \pmod{p}$ перед підсумовуванням перетворюється на послідовність двійкових символів.

Сторона A, отримавши повідомлення у формі Y_b та C, відновлює його:

$$M = (Y_b^{k_a} \pmod p) \oplus C.$$

Алгоритм Діффі-Хеллмана може бути використано задля розподілу ключів (генерування секретного ключа), але його не можна використовувати для шифрування повідомлення.

Згідно алгоритмом Діффі-Хеллмана, учасники інформаційного процесу A та B домовляються щодо значення великого простого числа p і простого дискретного кореня цього числа.

Сторона A обирає випадкове число k_a, а сторона B – випадкове число k_b у такий спосіб, щоби виконувалися умови

$$1 < k_a < p - 1 \quad \text{та} \quad 1 < k_b < p - 1.$$

Числа k_a та k_b тримаються сторонами A та B в секреті. Сторони A та B формують відкриті ключи за правилами

$$Y_{a,b} \equiv a^{k_{a,b}} \pmod p.$$

Після обміну несекретними ключами Y_a та Y_b сторони обчислюють значення секретного числа K:

$$K \equiv Y_a^{k_b} \pmod p \equiv a^{k_a k_b} \pmod p; \quad K \equiv Y_b^{k_a} \pmod p \equiv a^{k_b k_a} \pmod p.$$

Здобуте число K для ймовірного зловмисника є секретним, оскільки розв'язання рівнянь Y_a та Y_b для великих чисел є неможливе. Алгоритм Діффі–Хеллмана можна поширити на випадок з трьома і більше учасниками [3]. У табл. 1. наведені порівняльні характеристики алгоритмів асиметричного шифрування.

Таблиця 1.

Алгоритм	Ключ	Призначення	Криптостійкість	Примітки
RSA	До 4096 біт	Шифрування та підпис	$2{,}7 \cdot 10^{28}$ для ключа 1300 біт	Заснований на складності задачі факторизації великих чисел. Включений до багатьох стандартів.
ElGamal	До 4096 біт	Шифрування та підпис	При одинаковій довжині ключа криптостійкість рівнозначна RSA, тобто $2{,}7 \cdot 10^{28}$ для ключа 1300 біт	Оснований на складній задачі обчислення дискретних логарифмів в кінцевому полі; дозволяє швидко генерувати ключі без зниження стійкості.
Diffie-Hellman	Рекоменд. 1024 біт	Підпис	Визначається трудністю обчислення дискретного логарифма в кінцевому поле	Базується на передбачуваній складності проблеми дискретного логарифмування; працює тільки на лініях зв'язку, надійно захищених від модифікації

Література

1. Алфьоров А.П., Зубов А.Ю., Кузьмін А.С., Черьомушкін А.В. Основи криптографії: Навчальний посібник. 3-тє вид., Испр. і доп. - М.: 2005. - 480с.
2. Баранов В.М. и др. Защита информации в системах и средствах информатизации и связи. Учебное пособие. – СПб.: 1996. – 111 с.
3. Захарченко М.В. Асиметричні методи шифрування в телекомунікаціях: навч. посіб. / М.В. Захарченко, О. В. Онацький, Л. Г. Йона, Т. М. Шинкарчук. – Одеса: ОНАЗ ім. О. С. Попова, 2011. – 184 с.

УДК 621.319

АНАЛІЗ ПРОТОКОЛУ OTR ШИФРУВАННЯ ДЛЯ ОБМІНУ МИТТЄВИМИ ПОВІДОМЛЕННЯМИ

Пилипенко Б.В., Голь В.Д., Правило В.В.
Державний заклад Інститут спеціального зв'язку
та захисту інформації НТУУ «КПІ», Україна
E-mail: dens1087@bk.ru

Analysis protocol otr encryption for instant messaging

This paper analyzes the encryption method for instant messaging protocol XMPP / Jabber. An interaction procedures correspondents in the application of this method.

В роботі проведено аналіз методу шифрування OTR, який використовується в програмних продуктах, призначених для обміну миттєвими повідомленнями, визначені його переваги та недоліки, запропоновані принципи функціонування.

Характерними складовими методу є: обмін ключам, аутентифікація абонентів, шифрування та перевірка справжності протилежної сторони.

Обмін ключами

OTR використовує протокол Діффі-Хеллмана для обміну ключами, який є першим практичним методом для отримання загального секретного ключа при спілкуванні через незахищений канал зв'язку.

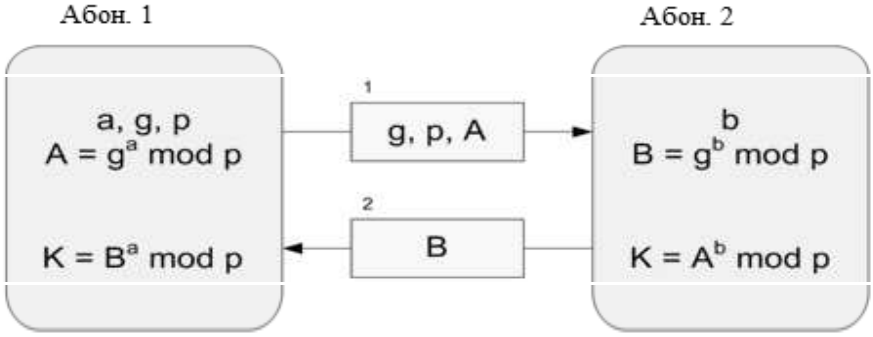


Рис. 1. Обмін таємними ключами.

При роботі алгоритму (рис. 1):

1. Кожна сторона генерує випадкове натуральне число a (b) – закритий ключ.

2. Спільно сторони встановлюють відкриті параметри p і g (зазвичай значення p і g генеруються на одній стороні і передаються іншій), де:

- p – є випадковим простим числом;

- g – є первісним коренем за модулем p (число g не повинно бути великим і зазвичай має значення в межах першого десятка).

3. Кожна сторона обчислює відкритий ключ A (B), використовуючи перетворення над закритим ключем:

$$A = g^a \bmod p; \quad B = g^b \bmod p.$$

4. Сторони обмінюються відкритими ключами з віддаленою стороною.

5. Кожна сторона обчислює загальний таємний ключ K, використовуючи відкритий ключ віддаленої сторони і свій закритий ключ:

$$K = B^a \bmod p; \quad K = A^b \bmod p.$$

K виходить рівним з обох сторін, тому що виконується властивість транзистивності:

$$B^a \bmod p = (g^b \bmod p)^a \bmod p = g^{ab} \bmod p = (g^a \bmod p)^b \bmod p = A^b \bmod p.$$

Аутентифікація.

Для цифрових підписів в OTR використовується алгоритм RSA, адже без додаткових засобів аутентифікації користувачі не могли бути впевнені, з ким саме вони згенерували загальний секретний ключ.

Рис. 1 Алгоритм аутентифікації абонентів.

Для відправника алгоритм аутентифікації буде наступним (рис. 2):

- взяти відкритий текст m;
- створити цифровий підпис s за допомогою свого секретного ключа {d, n}:

$$s = S_a(m) = m^d \bmod n$$

- передати пару {m, s}, що складається з повідомлення і підписи.

Для одержувача алгоритм аутентифікації складається з:

- приймання пари {m, s};
- приймання відкритого ключа {e} від відправника;
- обчислення прообразу повідомлення з підпису:

$$m' = P_s(s) = s^e \bmod e$$

- перевірки справжності підпису (незмінності повідомлення), порівнянням m і m'.

Шифрування.

Для шифрування в OTR застосований блоковий шифр AES. Цей алгоритм добре проаналізований і зараз широко використовується, будучи одним з найпоширеніших алгоритмів симетричного шифрування, оскільки 128-бітове шифрування AES наразі є досить надійним.

Перевірка справжності протилежної сторони.

Протокол Socialist Millionaire Protocol (SMP) використовується в OTR для перевірки справжності протилежної сторони, знаючи якусь загальну таємницю. Даний протокол дозволяє упевнитися в тому, що учасники знають якусь загальну інформацію (пароль, відповідь на питання відома тільки їм) не розголошуючи її напряму, не обмінюючись якимись її ознаками, що можуть бути використані сторонньою людиною, що знаходиться нібито в середині системи. Man in the middle, MITM-атака – ситуація, коли сторонній (атакуючий) здатний читати і видозмінювати по своїй волі повідомлення, якими обмінюються кореспонденти, причому жоден з останніх не може здогадатися про його присутності в каналі (рис. 3).

Рис. 2. MITM-атака.

OTR використовує SMP для порівняння інформації двох учасників – ідентифікаторів сесії, які представляють собою відбитки публічних ключів учасників і власне самої «таємниці».

Отже виходячи з вище описаного, метод OTR шифрування дає досить високу надійність, так як обмін ключами відбувається за допомогою протоколу Діффі-Хеллмана, внаслідок чого отримується загальний таємний ключ при використанні відкритого каналу передачі. Також застосовується алгоритм аутентифікації абонента та використовується досить стійкий алгоритм шифрування і виконується перевірка справжності протилежної сторони. Але зазначений метод має суттєвий недолік, а саме, він є вразливим до MITM-атак, за допомогою яких можна скомпрометувати сервер, через який проходять повідомлення і таким чином получити доступ до переписки. Боротьба с цим недоліком можлива шляхом створення власного сертифікаційного центру (серверу), який буде видавати відкриті ключі для аутентифікації та здійснювати інші процедури, що пов’язані із використанням спільної (публічної) інформації.

Таким чином, можна вважати, що метод OTR шифрування є досить надійним і можливим для використання в відкритому програмному забезпеченні для захищеного обміну миттєвими повідомленнями, але за умови використання власного сертифікаційного центру (серверу). В інших випадках є ризик того, що до переписки буде наданий доступ стороннім особам.

Література

1. OTR шифрування [електроний ресурс]: https://habrahabr.ru/post/149591.
2. Енциклопедія OTR шифрування [електроний ресурс] : http://jabberworld.info/OTR.

УДК 621.391

АНАЛИЗ ОСНОВНЫХ ПРОТОКОЛОВ АРХИТЕКТУРЫ IMS

Романов А.И., Верес Л.А., Явися В.С.
Інститут телекомунікаційних систем НТУУ «КПІ»
E-mail: aned@i.ua

Analysis of the main protocols of the IMS architecture

Bringing existing networks in line IMS concept requirements can significantly increase the efficiency of the existing telecommunications environment. It should seek to reduce the number of protocols used, increasing their functionality, as well as identify opportunities for their modernization in the direction of solving problems to ensure the specified quality of service, bandwidth and reliability.

Приведение существующих сетей в соответствие требованиям концепции IMS позволяет значительно повысить эффективность существующей телекоммуникационной среды. При этом необходимо стремиться к уменьшению числа используемых протоколов, повышению их функциональности, а также определению возможностей по их модернизации в направлении решения задач обеспечения заданного качества обслуживания, пропускной способности и надежности функционирования.

IMS (IP Multimedia Subsystem) - это развитие концепции сетей NGN по переходу к сетям All-IP для обслуживания мультимедийного трафика.

Изначально IMS разрабатывалась только как SDP (Service Delivery Platform) - мультимедийная платформа предоставления услуг. Но позднее IMS превратилась в архитектуру, полностью контролирующую процесс обслуживания заявок, поступающих из сетей доступа, построенных на базе различных технологий.

Основным отличием IMS от NGN является изменение структуры уровня управления. В связи с тем, что Softswich разных производителей не обеспечивали согласованной работы в процессе решения задач управления, в IMS они были заменены на совокупность серверов, реализованных в виде CSCF. Кроме того, уровень доступа и уровень магистральной транспортной сети в IMS были объединены и реализованы в виде одного уровня, в отличие от NGN, где эти уровни отделены друг от друга. Такой подход позволил уменьшить число используемых протоколов в центральной части сети.

В архитектуре IMS используются следующие основные протоколы:

- протокол инициирования (управления) сеансом – SIP;
- протокол описания сеанса – SDP;
- транспортные медиа протоколы, такие как RTP і RTCP;
- протоколы управления медиа - MEGACO/H.248
- протокол аутентификации Diameter

Дадим характеристику используемым протоколам.

SIP (Session Initiation Protocol) – протокол установления и завершения пользовательского интернет-сеанса, включающего обмен мультимедийным

содержимым. Это основной сигнальный протокол архитектуры IMS. Принцип построения сети на базе данного протокола представлен на рис. 1

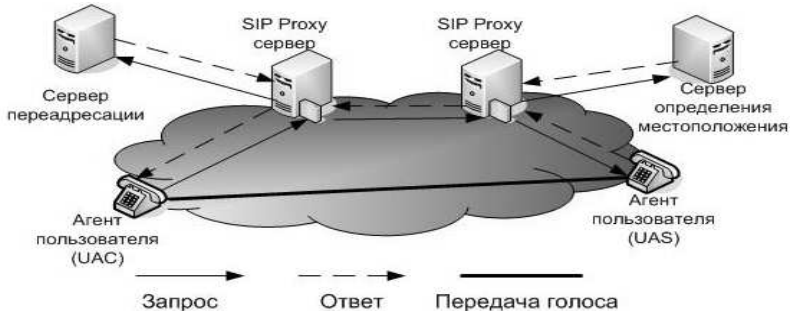


Рис. 1.

Протокол SIP имеет клиент-серверную архитектуру. Клиент выдаёт запросы, с указанием того, что он хочет получить от сервера. Сервер принимает и обрабатывает запросы, выдаёт ответы, содержащие уведомление об успешности выполнения запроса или об ошибке.

Обслуживание вызова распределено между различными элементами сети SIP. Основным функциональным элементом, реализующим функции управления соединением (кроме маршрутизации), является абонентский терминал.

Структура сообщений протокола SIP имеет следующий вид (рис.2):

Стартовая строка	Заголовоки	Пустая строка	Тело сообщения

Рис. 2.

Стартовая строка – это начальная строка любого SIP-сообщения. Если сообщение является запросом, в ней указывается тип запроса, адресат и номер версии протокола. Если сообщение является ответом на запрос, в ней указывается номер версии протокола, тип ответа и его короткая расшифровка.

Заголовки сообщений содержат информацию, необходимую для обработки информации об отправителе, адресате и пути следования.

Тело сообщения содержит описание сеансов связи. Не все запросы содержат тело сообщения (например, запрос BYE). Но все ответы содержат тело сообщения в обязательном порядке.

Достоинствами протокола являются: простота (включает в себя только шесть функций), обеспечение персональной мобильности пользователей, масштабируемость сети, взаимодействие с другими протоколами сигнализации, интеграция в стек существующих протоколов Интернет.

Протокол SDP (Session Description Protocol) - сетевой протокол прикладного уровня, предназначенный для описания сессии передачи потоковых данных [1]. Сессия SDP может поддерживать несколько потоков данных. В протоколе SDP определены аудио и видео данные, данные управления и приложений.

Недостаток SDP - в нём не хватает механизмов согласования параметров сессии между оконечными устройствами (например, формат данных, в котором будет осуществляться обмен). Поэтому поля протокола SDP включаются в сообщения протокола SIP. То есть, протокол SDP дополняет процесс управления вызовом, выполняя функции описания параметров медиа-сессии.

В отличии от сигнальных протоколов (SIP, SDP), протокол RTP (Real Time Transport Protocol) обеспечивает сквозную передачу в реальном времени мультимедийных данных, таких как интерактивное аудио и видео. Он реализует распознавание типа трафика, нумерацию последовательности пакетов, работу с метками времени и контроль передачи.

Пакет RTP включает в свой состав фиксированный заголовок, необязательное расширение заголовка переменной длины и поле данных.

Протокол RTP работает совместно с RTCP, который используется для передачи служебной информации о качестве услуг и возникновении перегрузок [2]. Совместное использование RTP и RTCP позволяет принимающему узлу располагать принимаемые пакеты в надлежащем порядке, снизить влияние неравномерности времени задержки пакетов на качество сигнала, обеспечить синхронизацию между аудио и видео.

Пакет RTCP начинается с фиксированной части, подобной фиксированной части информационных пакетов RTP, за которой следуют структурные элементы, имеющие переменную длину.

Протоколы управления медиа MEGACO/H.248 обеспечивают взаимодействие шлюзов, преобразующих голосовой трафик сетей с коммутацией каналов в пакетный трафик сетей с коммутацией пакетов.

Протокол Diameter обеспечивает решение задач аутентификации, авторизации и учета (Authentication, Authorization, Accounting - AAA) [3]. Он широко используется в IMS-архитектуре для обмена AAA-информацией между IMS-объектами.

Литература

1. https://ru.wikipedia.org/wiki/Session_Description_Protocol.
2. http://opds.sut.ru/old/electronic_manuals/itm_sait/tema71.htm.
3. https://www.ibm.com/developerworks/ru/library/wi-diameter/.
4. On extending open source IMS platform for integrated IPTV and VoIP services over IPv6 DATASET · JANUARY 2012.
5. Investigation IMS architecture According to Security and QoS context © AJMAL MUHAMMAD, March 2014. © RAJA MUHAMMAD SHAMAYEL ULLAH, March 2014.
6. https://ru.wikipedia.org/wiki/IMS_(%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D1%81%D0%B2%D1%8F%D0%B7%D1%8C).
7. http://www.iksmedia.ru/articles/4128111-Bezopasnost-i-frodkontrol-v-setyax. html
8. «Журнал сетевых решений/LAN», № 12, 2000.
9. «ПРОБЛЕМИ ТЕЛЕКОМУНІКАЦІЙ 2015 року» - Верес Л.А., Семендяк Е.С./Виды интерфейсов и их функции в архитектуре IMS.

УДК 004.7

ВИКОРИСТАННЯ ПРОГРАМНО-ВИЗНАЧЕНИХ МЕРЕЖ ДЛЯ МОДЕРНІЗАЦІЇ ІТ-ІНФРАСТУКТУРИ МОБІЛЬНОГО ЗВ'ЯЗКУ

Міночкін Д.А.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: dmytro.minochkin@gmail.com

Software defined network deployment for mobile communications IT infrastructure enhancement

The basic trends of software defined networks (SDN) are summarized. Possibilities of SDN deployment for mobile communications IT infrastructure upgrade are discussed.

Основою хмарних обчислень є принципи централізації і віртуалізації серверів, як результат зміни підходу до зберігання даних і використання програмного забезпечення. Тому, актуальним є напрям розвитку хмарних обчислень шляхом створення програмно-визначених мереж (SDN), централізації і віртуалізації управління мережею в хмарі. Після становлення SDN в центрах обробки даних (ЦОД), розгортання SDN переросло в Network as a Service (NaaS - мережа як послуга) - модель, яка пропонується клієнтам програмно визначених центрів обробки даних. Значна частина прибутків хмарних ЦОД буде припадати саме на послуги NaaS, і їх розмір буде збільшуватись (Рис. 1.) [1].

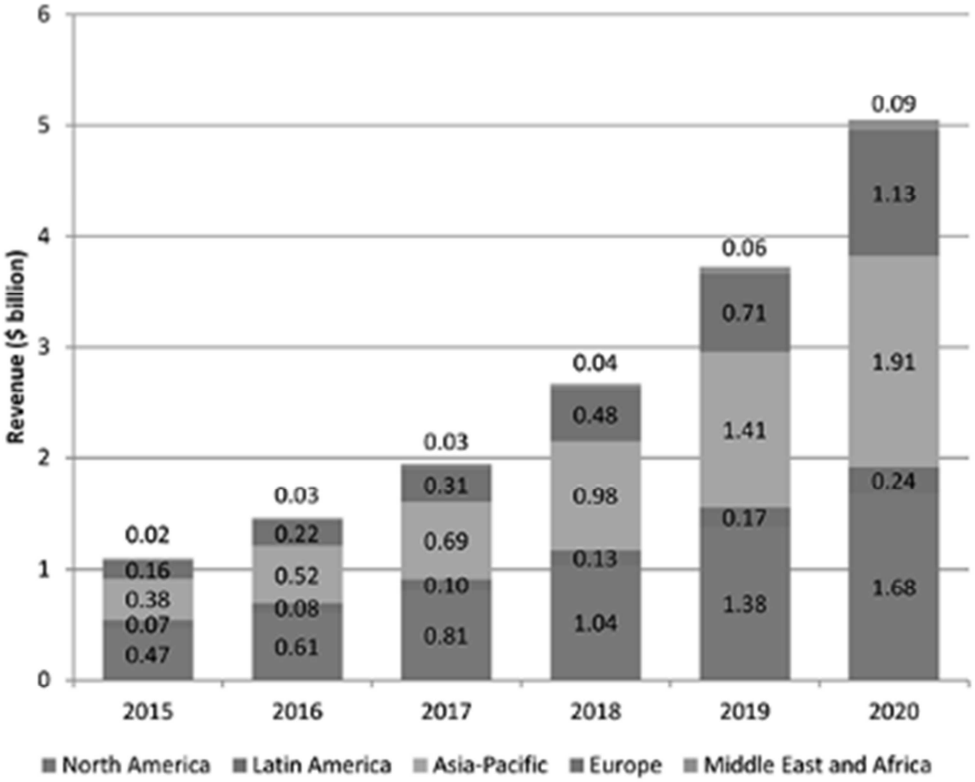


Рис.1 Прогноз розвитку ринку SDN.

Для модернізації ІТ-інфраструктури операторів мобільного зв’язку необхідно провести аналіз можливості використання технології SDN.

Перевагами SDN, по-перше, є зменшення потреби в технічних спеціалістах і, як результат, скорочення капітальних і експлуатаційних витрат оператора. По-друге, SDN забезпечує швидку взаємодію сервісів, оскільки дані програмуються сервісами віддаленого контролю (контролерами) і додатками. По-третє, SDN трансформує мережу в обчислювальний домен і переймає все більше практик стандартизації, які можна застосувати до комп'ютерів і програмного забезпечення [2].

Основною метою використання SDN є їх здатність швидко впроваджувати мережні інновації та радикальне спрощення і автоматизація процесу управління великими мережами.

З переходом ІТ-інфраструктури операторів мобільного зв’язку на використання хмарних ЦОД [3] тільки розгортання SDN може забезпечити своєчасність та автоматизацію надання мережевих з’єднань для елементів ЦОД та уніфікацію комунікацій оператора.

Обчислювальні ресурси в хмарних ЦОД створюються автоматично в режимі реального часу. Типове управління мережею з доступом до кожного мережевого елемента здійснюється набагато повільніше. Збої в роботі мережі можуть мати широкі наслідки, а вплив змін у мережі досить складно спрогнозувати. Відділення мережі від обчислювальної нестійкості і надання тільки плоских статичних сервісів зв'язку є одним з підходів вирішення цієї задачі.

Проте, хмарні ЦОД створюють нові вимоги до базової мережі. Наприклад, трафік від різних клієнтських сервісів повинен бути сегрегованим як для підвищення безпеки, так і для поліпшення продуктивності. Різні мережеві функції, такі як Firewall, системи розпізнавання Інтернет-трафіку і балансування навантаження повинні бути додані на вимогу клієнта і відповідно до його трафіку.

Таким чином, мережеві функції повинні бути тісно пов'язані з обчислювальним функціоналом, так як мережева політика повинна відповідати обчислювальній політиці, і звичайних статичних параметрів мережі стає недостатньо. Поширеним рішенням цієї задачі є розгортання SDN для динамічного конфігурування статичної мережі. Наприклад, VSwitch [4] (програмний комутатор з відкритим кодом) дозволяє динамічно маршрутизувати пакети для кожного сервера від віртуальних машин по різним статичним шляхам, визначеним в мережі. Менеджер ЦОД управляє інтерфейсом прикладного програмування (API) для застосування нових вимог до підключення до мережевого контроллера при внесенні змін до обчислювальних даних. Мережевий контролер може використовувати інтерфейс API щоб застосувати вимоги щодо забезпечення мережевого доступу і політики до програмного комутатора VSwitch.

Для підтримки внутрішніх бізнес процесів оператори зв’язку використовують інтерактивні медіа-додатки, такі як, наприклад, відео-конференції або віддалене робоче місце, які вимагають якості

обслуговування (QoS) в мережі, що гарантує їх продуктивність. Для цих додатків критично QoS і воно повинно підтримуватися в наскрізному режимі на основі глобальної мережевої політики, що робить процес розгортання і конфігурації складним. Отже, існуючі реалізації QoS в першу чергу обмежені специфікацією QoS, що базується на статичних рішеннях і частково на мережевому аспекті.

Для мережевих інфраструктур на сьогодні не існує ефективного способу ідентифікацій процесів, що вимагають QoS, і політик, які можна застосувати до кожного з них. Виділення ресурсів QoS також має бути динамічно адаптовано для задоволення різних потреб трафіку і чутливих до QoS робочих процесів. Використання SDN може допомогти автоматизувати QoS-конфігурацію всієї мережі для уніфікованих комунікацій. Також за допомогою використання SDN можливе не тільки надання необхідного QoS, а й масштабування використовуваних ресурсів. У разі неприйнятності, стан мережі може бути проаналізований в режимі реального часу і автоматично можуть бути вжиті необхідні заходи [5].

Таким чином, проведений аналіз показує можливість міграції мережевої інфраструктури операторів мобільного зв'язку на SDN. Розглянуті задачі, які можуть виникнути в процесі функціонування оператора мобільного зв'зку і погано вирішуються за допомогою діючих мереж. Доведено, що використання SDN може вирішити та автоматизувати поставлені задачі.

Література

1. SDDC Market Report 2015-2020 [Електронний ресурс] // Visiongain. – 2015. – Режим доступу до ресурсу: https://www.visiongain.com/Report/1457/Software-Defined-Data-Centre-(SDDC)-Market-Report-2015-2020
2. D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, S. Uhlig. Software-Defined Networking: A Comprehensive Survey // Proceedings of the IEEE 103 (1): pp. 14-76
3. Кравчук С. О. , Міночкін Д. А. Застосування розподілених обчислень в телекомунікаційних системах / С. О. Кравчук, Д. А. Міночкін. // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – 2015. – №50. – С. 41–44.
4. Why openvswitch? [Електронний ресурс] // Openvswitch. – 2015. – Режим доступу до ресурсу: https://github.com/openvswitch/ovs/blob/master/WHY-OVS.md
5. P. Kazemian, M. Chang, H. Zeng, G. Varghese, N. McKeown, and S. Whyte. Real-time Network Policy Checking using Header Space Analysis. In USENIX Symposium on Networked Systems Design and Implementation (NSDI), 2013.

УДК 621.3

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ PON В ЯКОСТІ МЕРЕЖІ СИНХРОНІЗАЦІЇ

Бірюков М.Л., Дяченко А.П.
Інститут телекомунікаційних систем НТУУ "КПІ", Україна
E-mail: dyachenko_a_p@ukr.net

The PON technology as perspective part of synchronization networks

Considered technology PON, principles of its work and a summary of the types of technology and the prospects of its use as telecommunications distribution network signals exact frequency.

Розвиток мережі Internet, у тому числі поява нових послуг зв'язку, сприяє збільшенню потоків даних, переданих по мережі, і змушує операторів шукати шляхи збільшення пропускної здатності та покращення якості переданої інформації. Саме тому провідною тенденцією розвитку сучасних телекомунікації є збільшення ролі оптичних технологій передавання інформації як в потужних магістральних трактах, так і на ділянці доступу зокрема.

Однією з перспективних оптичних технологій є технологія пасивної оптичної мережі – ПОМ (PON – Passive Optical Network). Новітні стандарти PON базуються на принципі WDM (Wavelength Division Multiplexing), який дає змогу суттєво підвищити ефективність використання оптичного волокна та підвищити пропускну здатність каналу. Крім того ПОМ, на відміну від інших оптичних технологій, вимагає набагато менших витрат на інфраструктуру оскільки дозволяє забезпечити широкосмугові швидкісні послуги без підсилення сигналів, тобто без залучення активних пристроїв. Активне обладнання в цій мережі є тільки на стороні оператора та абонента.

Технологія ПОМ активно розвивається і має декілька різновидів (Таблиця 1). Якщо перші реалізації були здебільшого орієнтовані на ATM та SDH, то зараз експерти працюють над системами PON наступного покоління – NG-PON2 [3] та XG-PON [2]. Основні цілі цих систем – збільшення швидкості, радіуса дії і кількості користувачів. Застосування WDM технологій сприятиме підвищенню потенціалу PON мереж до 40/100 Гбіт/с відповідно [4].

З впровадженням новітніх технологій і послуг, зокрема бездротового доступу – Wi-Fi, 2G-5G за наявності багатьох операторів та малих і дуже малих стільників (мікро– та фемто– стільників), передача даних висуває високі вимоги до транспортних мереж і зокрема параметрів синхронізації. Одним з важливих питань розвитку та впровадження є синхронізація БС (eNode-B) з високим ступенем точності частоти (<16 ppb) [4] і висока точність синхронізація у часі в межах від 1 до 0,5 мкс [5] в зв'язку з необхідністю забезпечення, наприклад, плавного передавання обслуговування (Handover), послуги з визначення точного місця

розташування абонента (Location) та ін.

Таблиця 1. Загальні характеристики різновидів технології ПОМ (PON)

Технологія PON	***A -PON (BPON)***	***E-PON***	***G-PON***	***XG-PON***	***NG-PON2***
Стандарт	G.983.x (x = 1-5)	IEEE 802.3ah,	ITU-T G.984.x (x = 1-7)	ITU-T G.987.1	ITU-T G.989.1
Базовий протокол	ATM	Ethernet IEEE 802.3	Ethernet* IEEE 802.3	Ethernet* IEEE	Ethernet* IEEE
Максимальна кількість ONU на волокно	32	16	64;128	32;64 (128;256)	≥256
Відстань, км	20	30(20)	20	20 (40;60)	≥60
Швидкість → / ← ,Гбіт/с	0,155/0,155 0,622/0,155 0,622/0,622	1/1	2,4/1,2 2,4/2,4	10/10;2,5	4÷8 × (2,5; 10/ 2,5;10)
Хвилі → / ←, нм	1550/1310 (1480/1310)	1550/1310 (1310/1310)	1550/1310 (1480/1310)	1260÷1280/ 1260÷2800	DWDM

Рекомендації МСЕ–Т передбачають використання трьох технологій доступу: цифрових абонентських ліній (DSL), РРЛ та ПОМ, відповідно до котрих розроблено гіпотетичні зразкові ланцюги (моделі) HRM–2a (РРЛ), HRM–2b – ПОМ та HRM–2c (DSL) [G.8261.1], які мають забезпечити синхронізацію мереж доступу. Гіпотетична базова модель HRM–2 з деталізацією для ділянці доступу з ПОМ – HRM–2b наведена на рис.1

В цьому призначенні PON майже єдина технологія яка завдяки відсутності проміжних вузлів, комутаторів, маршрутизаторів, шлюзів тощо може забезпечити високу пропускну здатність і високу якість високоточної синхронізації в умовах асинхронного засобу передавання пакетами:

- невеликої та сталої затримки передавання пакетів,
- незначних флуктуацій на фізичному рівні та незначної дисперсії часу прибуття пакетів на канальному рівні,
- наявності в обладнанні OLT, а зараз і ONU стандартних інтерфейсів синхронізації (точки Т3 та Т4 на рис.1), які відповідають вимогам [G.703] стиків для підключення обладнання мережевої синхронізації (E12; 2,047МГц, 10МГц, PTP, ToD – час доби),
- сталої топологічної архітектури, яка має структуру дерева та можливість резервування.

Слід зазначити, що гіпотетична базова модель HRM–2 визначає лише обмеження на ділянці власно до обладнання OLT (точка Т3) та має припущення, що кінцеве обладнання, яку приєднується до ONU (точка Т4), має функціональні можливості веденого пакетного генератора. Саме параметри передавання ділянки ПОМ залишаються для подальшого вивчення [G.8261.1].

Таким чином, при вивченні якісних показників частотної синхронізації

дослідженню підлягає одно направлена ділянка ПОМ, а саме HRM–2b між (PON in) та (PON out) яка має забезпечити одно направлене передавання на хвилі 1310 нм за протоколом PTPv2 (IEEE1588) або синхронного Ethernet (SyncEth). В разі фазової та часової синхронізації в структурі ПОМ має використатись двосторонній протокол PTPv2 та PTPv2+ SyncEth.

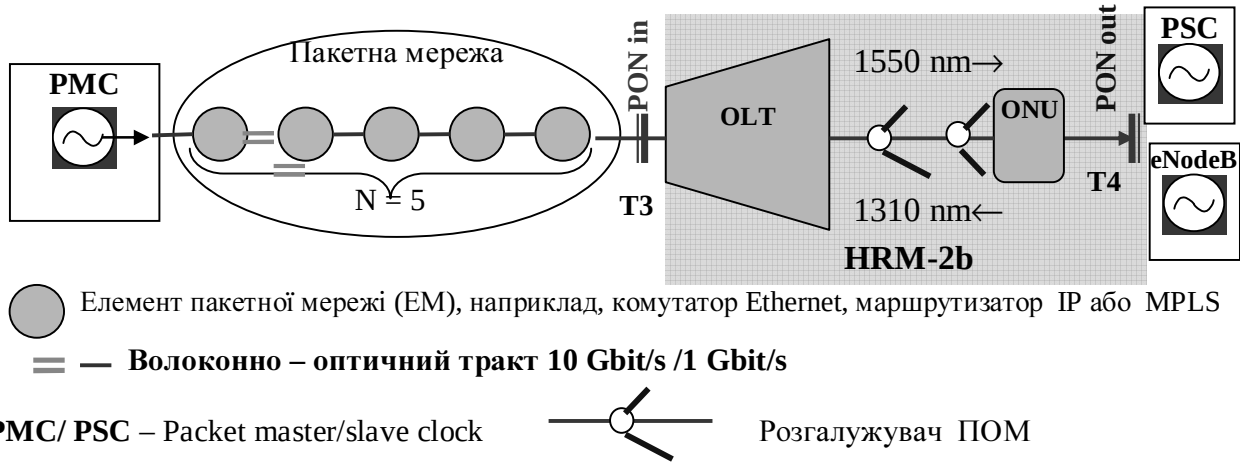


Рис. 1 Гіпотетична базова модель для ділянці доступу з ПОМ – HRM–2b.

Деякі попередні висновки, ґрунтовані на вимірюваннях обладнання різних постачальників, зокрема показують прямо пропорційну залежність розміру PDV (дисперсії затримок пакетів) від навантаження, розміру пакетів, швидкості передавання [7]. Але про все те ПОМ стає більш прийнятною технологією для надання послуг мережам наступного покоління.

Література

1. Бірюков М.Л., Стеклов В.К., Костік Б.Я. Транспортні мережі телекомунікацій: Системи мультиплексування: Підручник для студентів вищ. техн. закладів; За ред. В.К. Стеклова. – К.: Техніка, 2005. – 312 с., іл.
2. ITU-T Recommendation G.987.1 (01/10) 10-Gigabit-capable passive optical networks. (XG-PON): General requirements.
3. ITU-T Recommendation G.989.1 (03/13) 40-Gigabit-capable passive optical networks. (NG-PON2): General requirements.
4. PON – оптичекие сети с пассивной оптической магистралью [Електронний ресурс]. Режим доступу до ресурсу: http://deps.ua/.
5. Всеукраинский проект UA.PON [Електронний ресурс]. Режим доступу: http://ic-line.ua/projects/ua-pon.
6. Access network systems for future mobile backhaul networks Nov. 6, 2012 Seiji Yoshida.
7. Illustration of Packet Delay Variation (PDV) over GPON (access network) technology. ITU-T COM 15 – C 1438 – E June 2015/ Daniel Ph. Venmani, Yannick Lagadec.

УДК 621.39

ОСНОВНІ ПРИНЦИПИ УПРАВЛІННЯ МЕРЕЖЕВИМИ РЕСУРСАМИ В АРХІТЕКТУРІ ПРОГРАМНО-ВИЗНАЧЕНИХ МЕРЕЖ

Штепа В.О., Латуха А.В.
Інститут телекомунікаційних систем НТУУ «КПІ»
E-mail: tx7.vic@gmail.com

Main principles of network resource management within Software-Defined Networking architecture

This paper describes best practices of deploying systems with resource management within Software-Defined Networking architecture. These principles can be used as basis for developing high performance Quality of Service systems. For such systems SDN architecture provides agile and swift network management.

Останнім часом спостерігається тенденція до бурхливого розвитку та швидкого проникнення в галузі телекомунікацій програмно-визначених мереж (SDN). Архітектура програмно-визначених мереж відповідає новому підходу “програмування” мереж передачі даних, що надає можливості для динамічного створення, керування, модифікації та управління поведінки мереж за допомогою відкритих інтерфейсів. SDN підкреслює роль програмних продуктів у функціюванні мереж через абстрактне розділення рівнів управління та передачі трафіку. Таке розділення надає можливість швидкого впровадження інноваційних рішень на обох рівнях.

Одним із головних елементів програмно визначених мереж є контролери.

Контролер - програмне забезпечення або окремий фізичний пристрій; виконує управління передачі трафіку через мережу, надсилаючи необхідні інструкції маршрутизаторам та комутаторам. Іншими словами контролер керує мережевими пристроями. Має так звані “північний” та “південний” інтерфейси. Північний інтерфейс відповідає за зв'язок із мережевими додатками, а південний — за зв'язок із мережевими пристроями.

На даний момент, стрижневим протоколом у реалізації SDN-мереж є протокол OpenFlow. Відповідно, мережеве обладнання, яке працює на рівні передачі даних (data plane) повинне підтримувати архітектуру OpenFlow-комутатора. Комутатор OpenFlow складається з однієї або декількох таблиць потоків (flow tables) та групової таблиці (group table), які відповідають за пересилання пакетів. Використовуючи протокол OpenFlow контролер може додавати, оновлювати або видаляти записи таблиці потоків як реактивно(у відповідь на надходження пакетів), так і проактивно (за наперед заданим мережевим адміністратором сценарієм). Кожна таблиця потоків в комутаторі складається із набору записів потоків. Комутатор реалізує конвеєрну передачу пакетів.

Як бачимо, таких підхід до побудови та забезпечення управління мереж

надає широкі можливості для гнучкої реалізації управління мережевими ресурсами.

При реалізації системи управління мережевими ресурсами найбільш ефективними факторами функціонування такої системи будуть:

1. Автоматизоване, але високоточне управління. Точність управління якістю обслуговування може базуватися на потоках, що надходять. Тобто, система здатна реалізовувати гранульованість на рівні комбінації «IP-адрес абонента»+«TCP-порт» (або з ще більшою гранульованістю, залежно від версії протоколу OpenFlow).

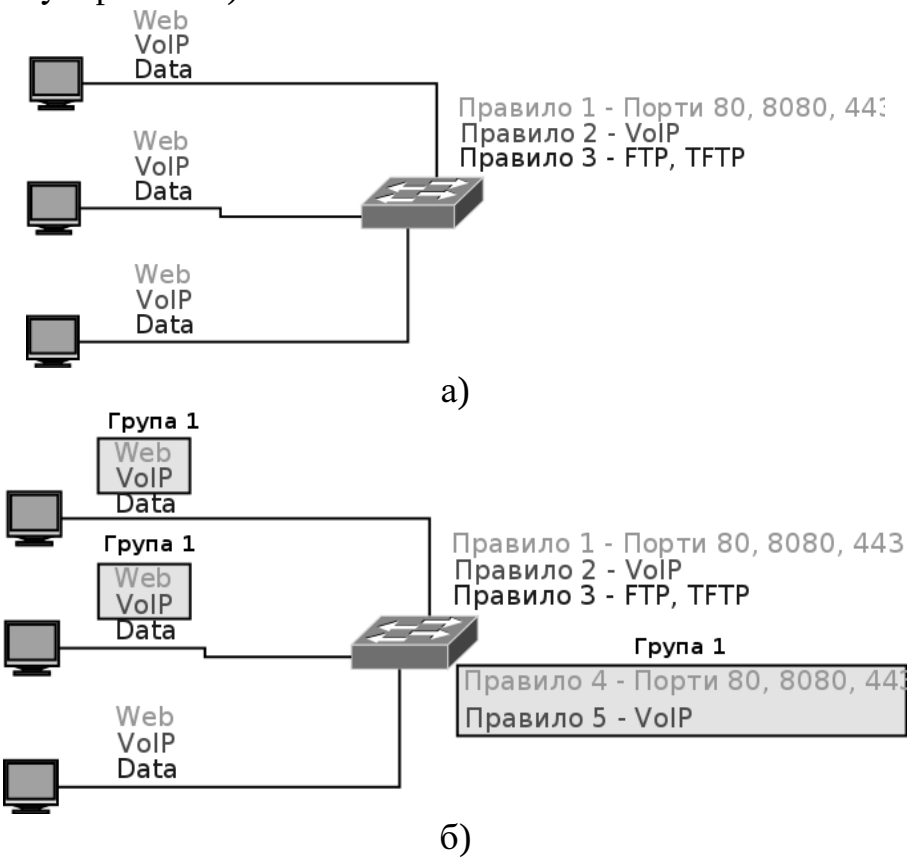


Рис. 1 Варіанти реалізації правил обслуговування на комутаторі з підтримкою OpenFlow.

Як видно з Рис.1.а, в такому випадку на комутаторі 1 можна виділити загальні правила для Web-трафіку від усіх абонентів (потоки з номерами портів 80, 8080, 443), створити високопріоритетну чергу для конкретних VoIP-додатків (Skype або інші сервіси) та низькопріоритетну чергу для додатків, які займаються резервуванням даних. Або, в разі необхідності, створити аналогічний розподіл правил обслуговування та пріоритету черг для кожного окремого абоненту або груп абонентів (Рис 1.б).

2. Адаптивність до динамічних навантажень. Даний фактор базується на можливості адаптації до стану мережі в реальному часі або (для зменшення перевантаження контролера та адекватної утилізації смуги пропускання мережі) із заданою затримкою певного проміжку часу. Стан мережі можливо отримувати використовуючи такі протоколи, як SNMP, RMON, NetFlow, IPFIX та інші (Рис. 2).

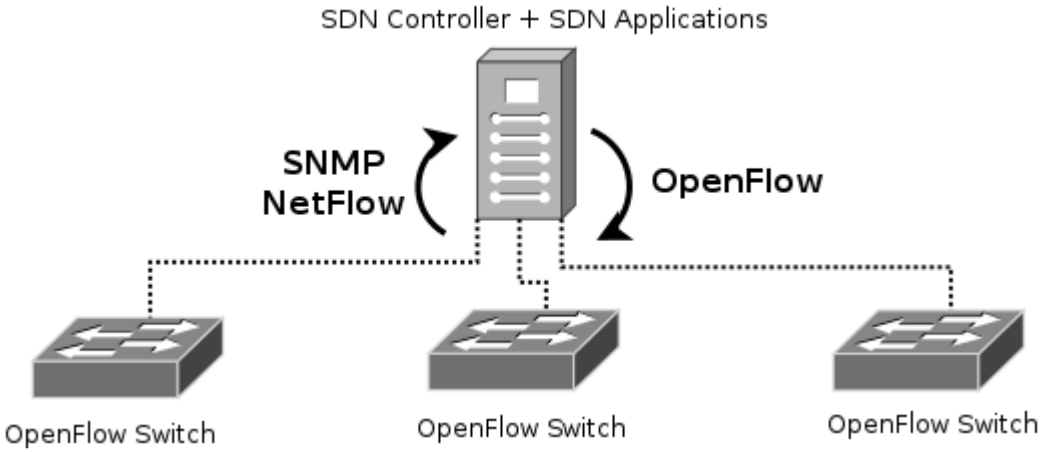


Рис. 2 Використання актуальної інформації про стан мережі
для забезпечення ефективних механізмів якості обслуговування

3. Ефективне використання ресурсів. Контролер повинен реалізовувати загальномережеву оптимізацію, виділяючи ресурси, необхідні для забезпечення відповідної якості обслуговування сервісів на базі аналізу глобальних тенденцій в мережі.

4. Можливість впровадження в існуючих мережах. Для повномасштабного забезпечення якості обслуговування під час інтеграції архітектури програмно-визначених мереж повинне братися до уваги вже існуюче обладнання та його функціональні можливості.

5. Підтримка високомасштабованих мереж. Обчислювальні потужності контролера повинні мати можливість бути збільшеними в разі відповідного розширення розмірів мережі.

Висновки. В роботі була розглянуті основні принципи при реалізації системи управління мережевими ресурсами в програмно-визначених мережах. Більш детальна реалізація зазначених механізмів буде наведена в магістерській дисертації на тему “Побудова високопродуктивних телекомунікаційних мереж на базі технології SDN та протоколу OpenFlow”.

Архітектура програмно-визначені мереж надає широкі можливості для ефективного та гнучкого управління як мережами в цілому, так і окремими наявними ресурсами. Для досягнення таких можливостей у програмно-визначених мережах використовується протокол OpenFlow.

Література

1. “OpenFlow Specification 1.5.1” - Open Networking Foundation, March 15, 2015.
2. OpenFlow-enabled SDN and Network Functions Virtualization // ONF Solution Brief // February 17, 2014.
3. Automated and Scalable QoS Control for Network Convergence // Wonho Kim, Puneet Sharma, Jeongkeun Lee, Sujata Banerjee, Jean Tourrilhes, Sung-Ju Lee, and Praveen Yalagandula // San Jose, CA, April 2010.

УДК 621.391

МОДЕЛЬ ПРОЦЕСУ УПРАВЛІННЯ ЗАХИСТОМ ВІД ПЕРЕНАВАНТАЖЕНЬ МЕРЕЖ ПЕРЕДАЧІ ДАНИХ

Романов О.І., Москвитіна А.О.
Інститут телекомунікаційних систем НТУУ «КПІ»
E-mail: a_i_romanov@mail.ru , anastasiia.moskvytina@ukr.net

Model of congestion protection in data networks

This paper presents method of congestion avoidance with RED techniques in packet-switching networks. Techniques for managing queues of packets are provided. The propose of the study to build a stochastic model of the traffic management RED type module.

Глобальні і локальні мережі схильні до перенавантажень. Це пов'язано з пульсаціями трафіку внаслідок зростання обсягу трафіку в одному або декількох напрямках зв'язку, виходу з ладу елементів мережі, переміщення абонентів і т.п. При цьому, досить складно визначити джерело виникнення перевантаження.

Одним з можливих шляхів боротьби з перевантаженнями є використання механізмів створення, розподілу и порядку обробки черги (Queuing Mechanism), які можуть бути класифіковані як:

- механізм FIFO (First-In, First-Out);
- черги пріоритетів (Priority Queueing);
- зважений алгоритм кругового обслуговування (Weighted Round Robin, WRR);
- конфігуровані черги (Custom Queueing).

Загальна постановка задачі стосовно управління чергами розглянута у [1]. У даній роботі представлений формалізований опис процесу обслуговування заявок і запропонована модель, що дозволяє запобігати перевантаження на ранніх етапах його виникнення.

Одним з найбільш ефективних алгоритмів, покладених в основу управління потоками черг, став алгоритм AQM (Active Queue Management), яскравим прикладом реалізації якого є алгоритм RED [2].

Суть ідеї закладається в тому, що алгоритм RED дозволяє відкидати пакети, що надходять у перезавантажений буфер з деякою вірогідністю, на основі оцінки середнього розміру черг [3]. Таким чином, він дозволяє контролювати навантаження в рамках черги і при виявленні перевантаження або стані близькому до перевантаження, здійснювати імовірнісне скидання пакетів.

Реалізація ідеї, закладеної в RED вимагає наявності формалізованої моделі, яка б адекватно відображала процес функціонування і дозволяла прив'язати всі змінні використовуваного математичного апарату. На рис.1 пропонується один з можливих варіантів такої моделі.

Модель на рис. 1 представлена одним маршрутизатором (комутатором) та двома персональними комп’ютерами. Генерацію трафіку здійснює один з ПК, другий його приймає. Алгоритм RED налаштовується у маршрутизаторі і припускає виконання таких основних блокових дій: відправка пакетів, обчислення

середньої довжини черги Q_{avg}, визначення границь порогових значень для Q_{avg}, розрахунок ймовірності скидання пакетів Pb та відкидання tail drop, формування черги *count* та прийом пакетів. Розглянемо ці етапи.

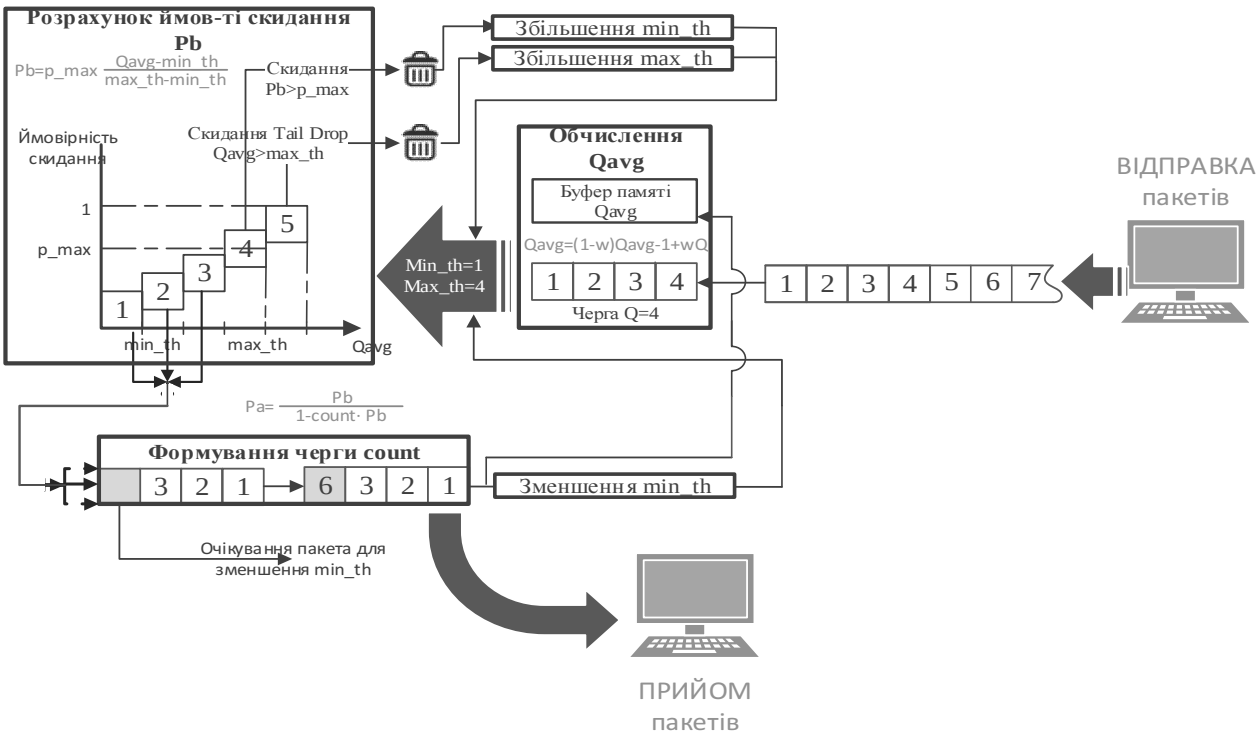


Рис. 1.

При надходженні пакетів до маршрутизатора розраховується значення середньої довжини черги Q_{avg}

$$Qavg = (1 - w)Qavq_{-1} + wQ, \quad (1)$$

де $Qavq_{-1}$ - попередній розмір черги, Q - поточний розмір черги, w - вага черги, пропорційна співвідношенню поточного і середнього розміру черги.

Значення $Qavq_{-1}$ зберігається у буфері пам'яті, як показано на рис. 1.

Після обчислення Q_{avg} маршрутизатор приймає рішення стосовно порогових значень для Q_{avg} . Мінімальне значення визначається як *min_th*, максимальне *max_th*. Якщо передбачуваний трафік буде мати пульсуючий характер (пікові перепади в навантаженні), значення *min_th* має бути досить високим, щоб забезпечити роботу мережі з високою якістю. Для трафіку високої пропускної здатності низьке значення нижнього порогу призведе до неприйнятно низькому завантаженні каналу.

Значення Q_{avg} має перебувати в межах мінімального та максимального порогів *min_th* і *max_th*. При розрахунку вірогідності скидання пакетів маршрутизатор виконує ряд перевірок.

- Якщо значення Q_{avg} більше максимального порога *max_th* - пакет відкидається за алгоритмом tail drop, а значення *max_th* збільшується;
- Якщо середній розмір черги Q_{avg} вище min_th, то пакет може бути відкинутий відповідно до ймовірності *Pb* (2). Відкинутий таким чином пакет призводить до збільшення значення *min_th*;

- Якщо середній розмір черги не вище *min_th*, то пакет проходить далі без затримок.

Якщо середнє значення черги перебуває в допустимих межах $min_th<Q_{avg}<max_th$, то пакети відкидаються відповідно до ймовірності *Pb*

$$Pb = \max_p \frac{Qavg - \min_th}{\max_th - \min_th}, \quad (2)$$

де *max_p* - максимальна ймовірність скидання. Значення *Pb* може змінюватися в межах [0; *max_p*], а величина *max_p* визначена порогом для ймовірності скидання *Pb*, при якому середня черга вже досягла свого максимального порога. Фактично відкидання пакету обумовлюється лише значенням *max_p*: якщо Pb більше max_p, пакет відкидається і мінімальний поріг збільшується.

Усі невідкинуті з попереднього етапу пакети додаються в лічильник кількості пакетів, які прийшли в чергу з моменту останнього скидання *count* - чим більше пакетів прийшло, тим вище ймовірність скидання. Значення *count* має бути достатнім для того, щоб знизити значення мінімального порогу *min_th*.

Ймовірність маркування або скидання пакетів обчислюється за допомогою лічильника *count* (3). Такий підхід гарантує, що RED не буде очікувати занадто довго, щоб відкинути пакет пропорційно навантаженню P_a [4]

$$Pa = \frac{Pb}{1 - count \cdot Pb}. \quad (3)$$

Алгоритм функціонування RED спрямований на таку реалізацію, яка дозволить відкидати пакети з дотриманням принципів «справедливого розподілу ресурсів», щоб уникнути глобальної синхронізації.

На основі запропонованого математичного апарату наступним етапом досліджень буде побудова імітаційних моделей, які могли би відобразити ефективність запропонованого методу боротьби з перенавантаженнями. Поточну модель пропонується доповнити кількома вузлами та розраховувати всі ймовірнісні показники, враховуючи передбачення на наступних ділянках мережі. Також планується наблизити експеримент до реального, організовуючи багатопотокову модель передачі даних.

Література

1. Москвитіна А. О. Управління перенавантаженнями у мережах передачі даних за допомогою організації черг / А. О. Москвитіна, А. О. Романов // Збірник тез VII Міжнародної науково-технічної конференції студентів та аспірантів «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем» - Київ, НТУУ «КПІ» 2015, с 149-151.
2. S. Floyd, V. Jacobson, Random Early Detection Gateways for Congestion Avoidance, IEEE/ACM Transactions on Networking 1 (4) (1993) 397–413.
3. Techniques for the hardware implementation of Random Early Detection mechanisms: pat. US006675220B1 USA / D. Bergamasco, T.J. Edsall, G. M. Morandin, K. McCloghrie. Publ. Jan. 6, 2014.
4. Киреева Н. В. Изучение алгоритма RED в среде NS-2 / Н. В. Киреева, М. А. Буранова, И. С. Поздняк // Методические указания к выполнению лабораторной работы. - «Поволжский государственный университет телекоммуникаций и информатики» (2014).

УДК 621.391

АНАЛІЗ І КЛАСИФІКАЦІЯ АТАК В МЕРЕЖАХ IP-ТЕЛЕФОНІЇ НА БАЗІ SOFTSWITCH CLASS V

Романов О.І., Гордашник Є.С.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: a_i_romanov@mail.ru; gordashnik@ukr.net

Analysis and attack classification in VoIP networks based on Softswitch class V

Ensuring security in VoIP network needs investigation of its vulnerabilities and attacks which pose a threat for stable network functioning. In this paper the most common and widespread attacks have been reviewed and analyzed. Classification and ensuring VoIP security method have been proposed.

Останнім часом оператори IP-телефонії, стрімко розвивають функціональність своїх послуг, надаючи користувачам все більш зручні та гнучкі можливості здійснення дзвінків, конференцій, колл-центрів. Разом з цим, з'явилося велика кількість вразливостей і атак, націлених на крадіжку особистих даних, перехоплення і запис розмов, доведення до відмови в обслуговуванні Softswitch, від яких провайдери послуг IP-телефонії все ще не захищені [1].

Існуючі види атак на безпеку мереж IP-телефонії можна розділити на 3 основні категорії [2]:

1. Атаки на сигналізаційну сесію - перехоплення, зміна тексту повідомлення і відправка його до Softswitch.
2. Атаки з метою розкриття змісту голосових повідомлень - перехоплення голосових потоків, запис і прослуховування.
3. Атаки на елементи мережі IP-телефонії, орієнтовані на відмову в обслуговуванні.

Структура мережі і принцип здійснення атак на елементи мережі IP-телефонії, показано на рис.1.

Розглянемо особливості проведення атак.

Перший клас атак - *атаки на сигналізаційну сесію*. Їх можна розглядати за наступними напрямками:

- руйнування сесії (TearingDownSessions)
- фальсифікація тіла повідомлення (TamperingwithMessageBodies)
- перехоплення реєстрації (RegistrationHijacking)
- голосовий фішинг і спам (SPIT - spamoverInternettelephony або VAM - voice / VoIPspam)

Принцип *руйнування сесії* (Tearing Down Sessions) полягає в тому, що хакери перехоплюють запити від різних абонентів і відправляють повідомлення BYE у відповідь (як якби він прийшов від проксі - сервера або іншого мережевого елемента). Це дозволяє завершити сесію достроково і обмежити доступ до послуг.

Атаки такого роду можуть бути запущені від окремих осіб, оскільки так набагато легше почати DoS атаку проти мережевих елементів і мережі в цілому, з набагато більш руйнівними і далекосяжними наслідками.

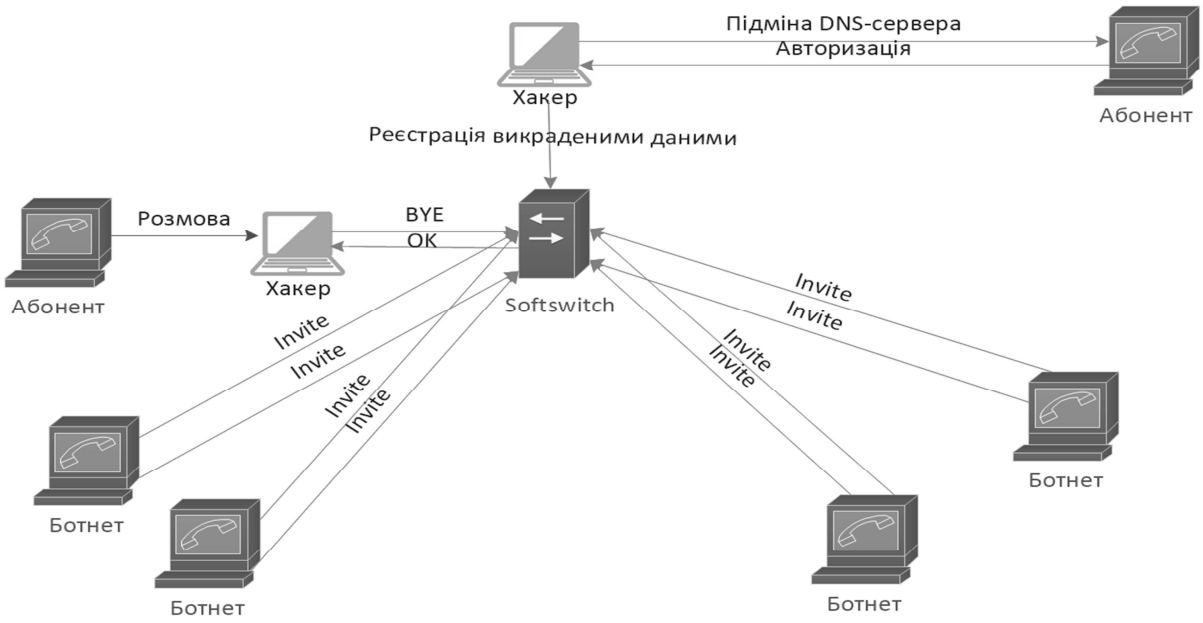


Рис.1.

Фальсифікація тіла повідомлення проводиться таким чином. Так як SIP повідомлення передаються в текстовому форматі (рис.2), тому шахраям абсолютно не обов'язково мати декодер для маніпуляції з повідомленнями. Просте захоплення повідомлення дає можливість втрутитися в роботу мережі. Як тільки хакер захопив повідомлення, тіло повідомлення і заголовки в протоколі SIP можуть бути змінені і використані зловмисником в своїх цілях.

Наприклад, хакер може захопити повідомлення INVITE (рис.2), що передається від абонента, і змінити його заголовок. Наприклад - адресу джерела, замінити своєю власною адресою. Це дозволяє хакеру підключатися до мережі, до якої він не має прав доступу. А далі, ініціювати сесію з іншими абонентами, видаючи себе кимось іншим.

```
INVITE sip:923406515540@192.95.30.203:5060;user=phone SIP/2.0
Allow: INVITE, ACK, BYE, CANCEL
Call-ID: sbcsipuac.2_66.33.182.50_b04sb13_1_1_2014111216265350_1758875847_402791
Contact: <sip:52710189@66.33.147.146:5060>
CSeq: 1001 INVITE
From: <sip:52710189@66.33.147.146:5060>;tag=1758875847_C
Max-Forwards: 70
P-Asserted-Identity: <sip:52710189@66.33.147.146:5060>
Privacy: none
To: <sip:923406515540@192.95.30.203:5060>
Via: SIP/2.0/UDP 66.33.147.146:5060;branch=z9hG4bK_1758875847_1957_1
Content-Type: application/sdp
Content-Length: 209
```

——— IP-адреса Softswitch

——— IP-адреса абонента, що ініціював виклик

Рис.2. Структура повідомлення Ivite.

Є й інші типи атак, в яких застосовується фальсифікація повідомлень. Так хакер може перехоплювати SMS-повідомлення та змінювати їх зміст. Це може бути особливо небезпечно, якщо повідомлення були послані з боку державних органів.

Перехоплення реєстрації (Registration Hijacking) дозволяє зловмисникові добути інформацію про користувача, яка міститься в SIP повідомленні. Вона в подальшому може бути використана для авторизації і аутентифікації в мережі і користування її сервісами.

Спроба реєстрації зловмисника буде виглядати, ніби абонент змінив своє місце розташування і шле новий запит реєстрації (повідомлення REGISTER). Після вдалої реєстрації, всі дані які були призначені абонентському пристрою користувача, будуть направлятися до зловмисника, що дозволить використовувати ресурс мережі користувачем, що не має на це прав. Такий вид атаки найбільш поширений в наші дні.

Голосовий фішинг і спам (SPIT - spamoverInternettelephony або VAM - voice / VoIPspam) може бути двох типів. Перший - користувач замість того, щоб працювати, слухає рекламу. Другій - абонент отримує пропозицію зателефонувати на «сервісний» номер (на кшталт Pay Pal) для уточнення деяких питань. У підсумку, оплата йде за збільшеним тарифам та розкриває персональні дані. SPIT і фішинг ще не стали масовим явищем, але вже помічені, і обсяги збільшуються.

Таким чином, для того щоб забезпечити режим нормального функціонування IP - мереж, необхідно застосовувати методи захисту, такі як, наприклад, шифрування даних і протидія DDOS-атакам. А для цього необхідно вивчення різних видів атак, їх класифікація та детальне формалізоване описання. У лабораторії кафедри Телекомунікацій проводиться збір і узагальнення такого виду інформації на макеті ділянки мережі з реальним обладнанням.

Виявлено, що однією з найбільш небезпечних видів атаки з метою виведення з ладу сервера є атака з використанням запиту Invite. Такий тип запитів найбільш трудомісткий, тому що змушує Softswitch звертатися до бази даних і порівнювати іноді цілий ряд параметрів. А це потребує часу до 300 мс. У порівнянні обробка запиту Register, займає 45 мс.

Література

1. An Improved SIP Security Mechanism of Softswitch Network // Q. Lu, C.G. Zhang – 2013 – 3с
2. A Comprehensive Survey of Voice over IP Security // Angelos D. Keromytis, Senior Member, IEEE - 2012 – 24с
3. A Comprehensive Survey of Security Issues and Defense Framework for VoIP Cloud // Ashutosh Satapathy, L. M. Jenila Livingston, School of Computing Science and Engineering, VIT University, Chennai - 600127, Tamil Nadu, India- 2015 – 13с

УДК 004.73+621.39

МЕТОДИ СЕЛЕКЦІЇ ПЕРЕВАНТАЖЕНЬ ТА ВІДМОВ МЕРЕЖНИХ ВУЗЛІВ

Харлай Л.О.
Державний заклад «Київський коледж зв'язку»
E-mail: Lharlay@i.ua

The method of selection of overloads and failures of network nodes

Further development of politics of traffic is application of the differentiated and integrated services it is dynamic allocation of stripe of key-in of channels of transmission between users taking into account their priorities instead of direction of all streams one by one or by a few locally-optimal routes. At such approach it is succeeded to avoid the periodic local overloads of routes, that were certain as optimal on the current stage, and on that all users directed the traffic.

Одна з проблем мереж – це ефективний контроль трафіку. Спостереження за потоком трафіку називається політикою трафіку [1]. Методи вирішення проблеми контролю трафіку ґрунтуються на застосуванні політики, що дозволяє гармонійно розподілити інформаційний потік. Провідні розробники мережевого устаткування намагаються утілити ідею використання політики контролю трафіку в технічні рішення. Як правило, реалізуються методи QOS (Quality of Service) і COS (Class of Service), які досить тісно зв'язані між собою.

У тих випадках, коли об'єм трафіку або затримки в мережі можуть зростати в межах 10–30%, розумно буде задіювати QoS/CoS-політику як спосіб контролю трафіку. В результаті застосування політики пріоритетів створюються марковані потоки трафіку. Алгоритм політики, наприклад, може визначити, що пакети, які згенеровані чутливими до затримок додатками, мають перевагу по доставці перед пакетами інших типів – обміну файлів або електронної пошти. Якщо ж виникне ситуація, коли частина пакетів в результаті перевантаження буде відкинута, то насамперед це трапиться з пакетами з низьким пріоритетом. Разом із забезпеченням достатньої смуги пропускання схема пріоритетів дозволяє здійснити доставку необхідного трафіку в пункт призначення.

Одним з раціональних шляхів управління трафіком (що вимагає значно менших витрат, ніж реалізація політики *QOS*) може служити динамічне управління ресурсами мережі – розділення смуги пропускання на декілька частин для конкретних потреб. У разі, коли зростає навантаження, пакети починають розміщуватися в буферній пам'яті мережевих вузлів, що приводить до затримок. Проте очевидне, на перший погляд, рішення збільшення об'єму буферної пам'яті – не приводить до поліпшення ситуації з перевантаженнями, а іноді може навіть погіршити її.

Тому подальшим розвитком політики трафіку є застосування диференційованих і інтегрованих послуг [1] – динамічний розподіл смуги пропускання каналів передачі між користувачами з урахуванням їх пріоритетів замість направлення всіх потоків поодинці або декількома локально-оптимальними маршрутами. При такому підході вдається уникати періодичних місцевих перевантажень маршрутів, які були визначені як оптимальні на

поточному етапі, і по яких всі користувачі направили свій трафік.

Таким чином, для реалізації політики трафіку з диференційованими послугами необхідно вирішувати задачу розподілу потоків між локально-оптимальними або квазіоптимальними маршрутами в реальному часі. Проте раніше доцільно проаналізувати процес формування сумарних потоків в парціальних каналах загальної мережі передачі даних.

Розглянемо модель процесу формування сумарного потоку в результаті накладення окремих потоків від різних джерел. Тут необхідно чітко розмежовувати поняття «Потік трафіку» і «процес в мережі». Потоки трафіку в сучасних цифрових мережах з пакетною комутацією найчастіше мають самоподібний характер, що доведено численними експериментальними дослідженнями. Процеси в мережах, такі, як пошук оптимальних маршрутів, формування і регулювання потоків трафіку, встановлення і розрив з'єднання, організація обміну даними усередині автономного сегменту мережі,між сегментами, можна розглядати як певні потоки заявок на обслуговування у відповідному вузлі, мережевому або термінальному.

У свою чергу, сучасні прилади маршрутизації, будь-то програмні маршрутизатори чи апаратні, мають можливість тільки статичного розмежування ресурсів каналу.

Розглянемо модель мережі пакетної комутації, у якій квитування пакетів здійснюється тільки між сусідніми вузлами. Невдало переданий пакет повторюється з вузла відправника. Це вимагає збереження копії пакета в буферній пам'яті передавального вузла до моменту одержання від сусіднього вузла позитивної квитанції про прийом пакета. Відсутність відгуку протягом тайм-ауту класифікується як утрата пакета, і передавальний вузол повторює пакет по тому ж самому або новому маршруту [1]. Розглянемо мережу, що складається з W вузлів комутації пакетів, пам'ять яких являє собою множину однорідних буферів. Канали зв'язку для простоти передбачаються абсолютно надійними, так що повторення передачі пакетів між сусідніми вузлами визначається лише зайнятістю буферної пам'яті вузла.

Припустимо, що в мережі передаються пакети R класів, маршрути яких задаються матрицями $\|P_{Ri}(r)\|$, де $P_{Ri}(r)$ ($R = \overline{1,\mathrm{W}}$; $i = \overline{1,\mathrm{W}}+1$; $\mathrm{r} = \overline{1,\mathrm{R}}$) – імовірність передачі пакета класу r з вузла R у вузол i ($P_{Ri}(r) + \ldots + P_{RW+1}(r) = 1$). Пакет класу r завершує обслуговування в мережі, залишаючи її з R-го вузла по каналу $(R, W + 1)$. Пакети надходять у мережу з R зовнішніх джерел з інтенсивністю $\Lambda_r = (r = \overline{1,R})$. Нехай $\lambda_{0i}(r) = \Lambda_r P_{0i}(r)$, тоді очевидно, що загальний потік, що надходить у мережу,

$$\Lambda = \sum_{r=1}^{R}\sum_{i=1}^{W}\lambda_{0i}(r). \qquad (1)$$

Як і раніше, передбачається, що потоки $\lambda_i(r)$, що надходять у вузол, є пуассоновськими.

Рівняння балансу потоків для вузлів розглянутої мережі має вигляд

$$\lambda_i(r) = \lambda_{0i}(r) + \sum_{R=1}^{W} \lambda_R(r)\pi_R(\lambda_R)P_{Ri} + \\ +\lambda_i(r)(1-\pi_i(\lambda_i)),\ i=\overline{1,W};\ r=\overline{1,R}, \tag{2}$$

де $\lambda_R = \sum_{R=1}^{W} \lambda_R(r); \pi_R(\lambda_R)$ – стаціонарна імовірність наявності вільного буфера в *R*-му вузлі мережі.

Система (2) може бути записана у виді

$$\lambda_i(r) = \frac{1}{\pi_i(r)}(\lambda_{0i}(r) + \sum \lambda_R(r)\pi_R(\lambda_R(r)P_{Ri}(r)). \tag{3}$$

Вводячи позначення $\gamma_i(r) = \lambda_i(r)\pi_i(\lambda_i), i=\overline{1,W}; r=\overline{1,R},$ і підставляючи $\gamma_i(r)$ в (2), одержуємо систему рівнянь балансу потоків для мережі з необмеженою пам'яттю у вузлах

$$\gamma_i(r) = \lambda_{0i}(r) + \sum_{R=1}^{W} \gamma_R P_{Ri}(r). \tag{4}$$

Останній вираз показує, що, зберігаючи баланс потоків, що пропускаються мережею, інтенсивності потоків у вузли з обмеженою буферною пам'яттю перевершують відповідну інтенсивність мережі з необмеженою пам'яттю в $1/\pi_i(\lambda_i)$ разів. При цьому число повторень передачі по каналах мережі (R,i) $R \neq i; R,i = \overline{1,W}$ можна вважати розподіленим по геометричному закону із середнім $1/\pi(\lambda_i)$. Останнє еквівалентно збільшенню відносної частоти відвідування центрів обслуговування моделі замкнутої мережі масового обслуговування при $F_i = 1 - \pi_i(\lambda_i)$. Таким чином, взаємовплив при міжвузловому квітіруванні виявляється у функціональній залежності $\pi_i(\lambda_i) = \Phi_i(\pi_i(\lambda_i),.....,\pi_W(\lambda_W))$.

Зазначена мережа досліджувалася за допомогою еквівалентної системи нелінійних рівнянь щодо ймовірностей зайнятості буферної пам'яті вузла

$$B_i = 1 - \pi_i(\lambda_i)\ ,\ i = \overline{1,W};\ B_i = f_i(B_1, B_2, \ldots\ldots, B_W)... \tag{5}$$

Система рівнянь розв'язується чисельними методами, наприклад, методом Ньютона, збіжність якого істотно залежить від вибору початкового наближення. Середній час затримки пакетів для розглянутої мережі визначається виразом (5), де

$$P_{0i} = \sum_{i=1}^{R} P_{0i}(r); \alpha_i = \lambda_i / \lambda_{0.}$$

В сучасних мережах пропускна здатність каналу є досить сталою величиною. Тому не враховуємо вплив пропускної здатності каналу на відносний час передачі пакетів. Параметром за яким можна судити про завантаженість мережі є: час затримки пакету в буфері маршрутизатора.

Література

1. Таненбаум Э., Уэзеролл Д. Компьютерные сети: 5-е изд. – СПб: Питер, 2012. – 960 с.
2. Столлингс В. Современные компьютерные сети. 2-е изд. – СПб.: Питер, 2003. – 783 с.

УДК 004.56.5

АНАЛІЗ МЕТОДІВ ЗАХИСТУ СЕРВЕРІВ ВІД РОЗПОДІЛЕНИХ *TCP SYN-FLOOD* АТАК

Нестеренко М.М., Романов А.О.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
Інститут спеціального зв'язку та захисту інформації НТУУ «КПІ», Україна
E-mail: nesterenko_nik@ukr.net, anton3329@gmail.com

Analysis methods of protection servers from distributed TCP SYN-flood attacks

The article presents one of the most common types of DDos-attacks on the server – TCP SYN-flood attack. The model and describes how to interact with the attacker's server during a DDos-attack. We analyzed the currently used methods of protection: TCP SYN Cookies, TCP RST Cookies, Floodgate, Random / Old Drop, SYN-Proxy, Stack Tweaking, Blacklisting.

Ефективна робота будь-якої організації не можлива без створення власної інфраструктури на базі сучасних інформаційних сервісів. Основою для реалізації відповідного сервісу є мережева операційна система на платформі якої розгортаються основні сервери такі, як *DNS*-, *mail*-, *FTP*- та *Web*-сервер. В умовах постійної конкуренції особливо гостро постає питання надання широкого спектру інформаційних послуг якість яких залежить від часу відклику та доступності серверів. Однак, останні дослідження в області комп'ютерної безпеки [1] вказують на постійний зріст та удосконалення мережевих *DDos*-атак, які в першу чергу направлені на збій в роботі (або блокування) інформаційних служб. Тому завдання оптимального конфігурування системи захисту серверів є актуальним.

Одним з основних типів *DDos*-атак є *TCP SYN-flood*, механізм проведення якого базується на використанні вразливостей протоколу *TCP*. Дана атака розрахована на обмеження кількості напіввідкритих *TCP*-з'єднань, яке задано по замовчуванню у вбудованому модулі *TCP/IP* мережевої операційної системи. Узагальнена схема проведення *TCP SYN-flood* атаки приведена на схемі рис. 1.

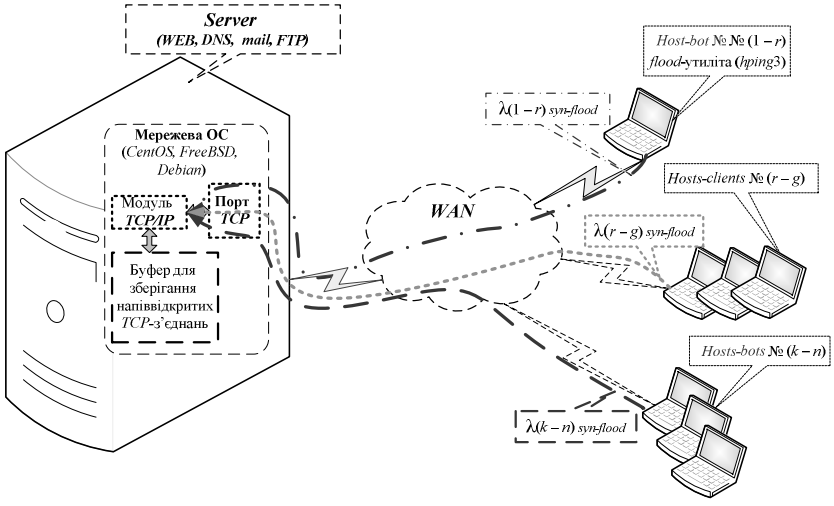


Рис. 1. Функціональна схема *TCP SYN-flood* атаки на Unix- сервер.

А саме, коли на сервер здійснюється *TCP SYN-flood* атака, то за рахунок збільшення інтенсивності *SYN*-запитів утворюється (та постійно зростає) черга з напіввідкритих *TCP*-з'єднань в стані *SYN RECEIVED* та як наслідок призводить до вичерпання ресурсу модуля *TCP/IP*, тобто сервер більше не може обробляти вхідні запити [2].

Для збільшення ефекту даного типу атаки боти використовують фіктивні *IP*-адреси для ускладнення процесу ініціалізації сервером (повторні перезапити) так, як згенерована *IP*-адреса може бути недосяжною. Дана операція також називається *SYN*-спуфінгом.

Необхідно відмітити, що деякі *TCP SYN-flood* атаки не завжди намагаються перезавантажити сервери, замість цього задачею є вичерпання всієї пропускної спроможності *Internet*-каналу [3], за рахунок повторних запитів збоку сервера при неотриманні відповіді від псевдо-клієнтів (ботів).

В свою чергу, процес повторної передачі буде ініціалізуватись з боку сервера за допомогою *SYN-ACK* запитів, до моменту отримання *ACK*-відповіді від клієнта. Тобто, пакет з флагом *ACK* з боку клієнта є підтвердженням на встановлення *TCP*-з'єднання з сервером (рис. 2 а).

Якщо сервер на який здійснюється атака не отримує відповідь від віддаленого хоста-клієнта, то він повторно робить перезапит (*SYN+ACK*-запит) до тих пір поки не наступить тайм-аут, а потім видаляє це напіввідкрите *TCP*-з'єднання з черги (рис. 2 б).

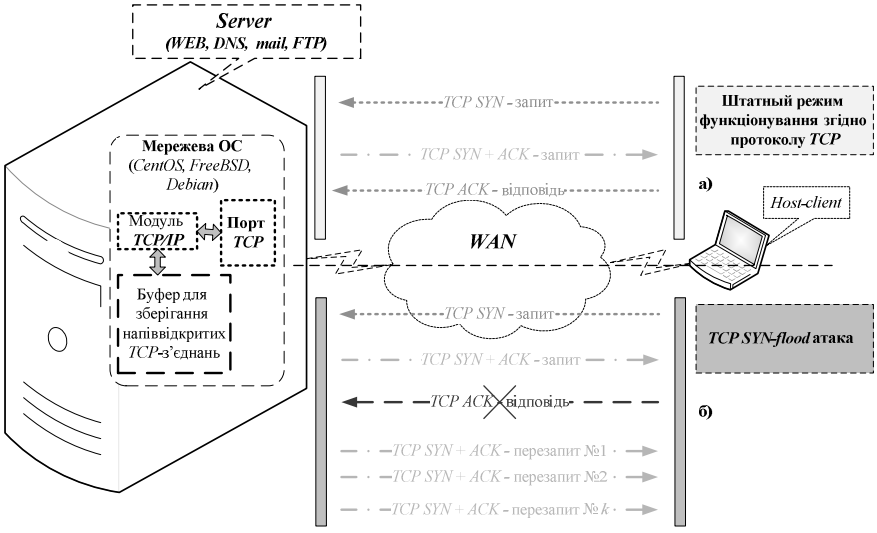


Рис. 2. Порядок проведення *TCP SYN-flood* атаки
при використанні вразливості протоколу *TCP*

На теперішній час відомі наступні методи протидії *TCP SYN-flood* атакам [4]:

- *TCP SYN Cookies* (блок управління передачею – *TCB* на сервері кодує порядковий номер і зберігає закодовану комбінацію у хеші, після чого відправляє *SYN-ACK* з закодованим *cookie* і закриває з'єднання. Якщо у відповіді *ACK* клієнта *cookie* співпадає то сервер відкриває *TCP*-з'єднання);

- *TCP RST Cookies* (сервер відправляє клієнту, який надіслав запит на *TCP*-з'єднання *SYN+ACK* пакет з невірними параметрами. У відповідності до специфікації протоколу *TCP* клієнт повинен надіслати *RST*-пакет. Якщо сервер

отримує від клієнта даний *RST*-пакет, то сервер додає клієнта до списку легітивних користувачів);

- *Floodgate* (фізичний або програмний засіб, який випадковим чином відкидає *TCP*-з'єднання);

- передмаршрутизаційна фільтрація/*Blacklisting* (маршрутизатори мережі контролюють всі *IP*-адреси відправників та відфільтровують пакети з неіснуючими *IP*-адресами);

- *Random / Old Drop* (видаляє напіввідкриті *TCP*- з'єднання випадковим чином або ті з'єднання встановлений ліміт яких вичерпано);

- *SYN-Proxy* (використовується додатковий *proxy*-сервер, призначенням якого є обробка *SYN* пакетів. Якщо *proxy*-серверу вдалось встановити *TCP*-з'єднання з клієнтом, то клієнт допускається до ресурсів сервера);

- *Stack Tweaking* (полягає в зміні налаштувань протоколу *TCP*, а саме:

- таймаут перед закриттям напіввідкритого *TCP*-з'єднання, максимально допустима кількість напіввідкритих з'єднань і час очікування *ACK*-відповіді від клієнта);

- *Blacklisting* (сервер не обслуговує запити від клієнтів, які потрапили в *blacklist*, як правило використовується з передмаршрутизаційною фільтрацією);

- мережеві системи виявлення вторгнень *IDS* (система виявлення та запобігання атак, яка комбінує в собі методи зіставлення по сигнатурам, засоби для інспекції протоколів і механізми для виявлення аномалій).

Однак, запропоновані методи в основному працюють по принципу відсікання запитів по інтенсивності, без додаткових механізмів перевірки легітимності запитів, або вимагають складних налаштувань збоку серверного обладнання.

В подальшому симуляцію атаки на *Web*-сервер (Apache) було проведено за допомогою утиліти *hping3*, яка дозволяє генерувати *SYN-flood* від неіснуючих *IP*-адрес, що обираються випадковим чином. В результаті перевірки завантаженості сервера було з'ясовано: процесор майже не задіяний, вільної оперативної пам'яті більше половини, отже фізичні ресурси сервера не були вичерпані, проте черга потоків в модулі *TCP/IP* була повністю зайнята, що призвело до непрацездатності сервісу на 80 порту.

На основі вище приведеного, розробка моделей та методик виявлення *flood*-атак вимагає визначення конкретних значень параметрів системи захисту при її конфігуруванні. А саме, динамічну зміну заданих по замовчуванню стекових змінних по протоколу *TCP/IP* у відповідних модулях мережевих операційних систем в залежності від кількості *SYN*-запитів.

Література

1. http://expert.com.ua/100780-issledovateli-check-point-otmetili-rost-ddos-atak-v-yanvare-2016-goda.html.
2. Инструменты безопасности с открытым исходным кодом /Хаулет Т. – М.: НОУ „Интуит" 2016. – 556 с.
3. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин. – М.: ФОРУМ, 2013. – 416 с.
4. Feinstein L., Schnackenberg D., Balupari R., Kindred D. Statistical Approaches to DDoS Attack Detection and Response. // DARPA Information Survivability Conference and Exposition.

УДК 621.39

ОЦЕНКА ПРОИЗВОДИТЕЛЬНОСТИ ТРАФИКА В СЕТИ MPLS С ИСПОЛЬЗОВАНИЕМ TRAFFIC ENGINEERING

Маньковский В.Б.
Научный руководитель: проф., д.т.н. Романов О. И.
Институт телекоммуникационных систем НТУУ «КПИ»
E-mail: mankovskij@yandex.ru

Evaluate the performance of MPLS network with the traffic engineering

One of the methods of increasing network performance is IP-networks on MPLS technology. A key feature of MPLS technology is the Traffic Engineering, which has a vital role to minimize packet delay through effective load balancing and network management. In this article, one of the important parameter of a network, in terms of performance was rated - time of a packet in a congested network MPLS-TE and conventional IP-network.

Одним из способов повышения производительности сети является IP-сетей по технологии MPLS. Ключевой особенностью технологии MPLS является Traffic Engineering, которая играет важную роль для минимизации задержки пакета за счет эффективного распределения нагрузки и управления сетью. В этой статье, рассмотрен один из важных параметров сети, с точки зрения производительности, - время передачи пакета в перегруженной сети MPLS-TE и обычные IP-сети.

В последнее время среда Интернет выступает в роли сети доступа в режиме реального времени для приложений, которые должны иметь минимально возможную временную задержку при передачи пакетов от источника к потребителю. Такие приложения оперируют данными, которые имеют малый размер пакета, но большую интенсивность передачи. Эти приложения требуют широкую пропускную способность канала для того, чтобы обеспечить необходимые задержки, и данный показатель не относится к повышению экономической эффективности.

В интерактивных приложениях при передачи трафика в реальном времени, общая задержка в одном направлении должна быть коротка, чтобы дать приложению состояния on-line. При превышении времени ожидании, приложения разрывают соединение в клиет-серверных архитектурах. Максимальное значение задержки порядка от 0,5 до 0,9 секунды требуется для достижения этой цели[1]. Согласно спецификаций Международного союза электросвязи (МСЭ) рекомендует задержку около 550 мс в одну сторону от начала линии до конца для высокоскоростного трафика.

MPLS стала ключевой технологии интеграции для осуществления передачи трафика данных по той же сети, и эта технология, которая играет важную роль в сетях следующего поколения, путем предоставления качества обслуживания (QoS) и TE (Traffic Engineering). В сети MPLS, LSPs (Label

Switched Path) устанавливаются из входного узла к узлу исходящего трафика до начала передачи. Каждый LSP может быть задан с функциями, которые включают ограничения и надежность по времени доставки [2]. Поэтому приложения, ориентированные на составление канал, могут воспользоваться "виртуальным соединением", установленным MPLS.

Для данного доклада была использована среда моделирования GNS3 для создания топологии сети, как показано на рис.1 для традиционных IP сетей и для MPLS сетей. Моделирование состоят из двух сценариев на представленных топологиях сети. Сценарий 1 на основе IP: сеть без TE (в составе протокола OSPF). Сценарий 2 на базе MPLS сети с TE. Результаты этого моделирования используются для сравнения между двумя сетями.

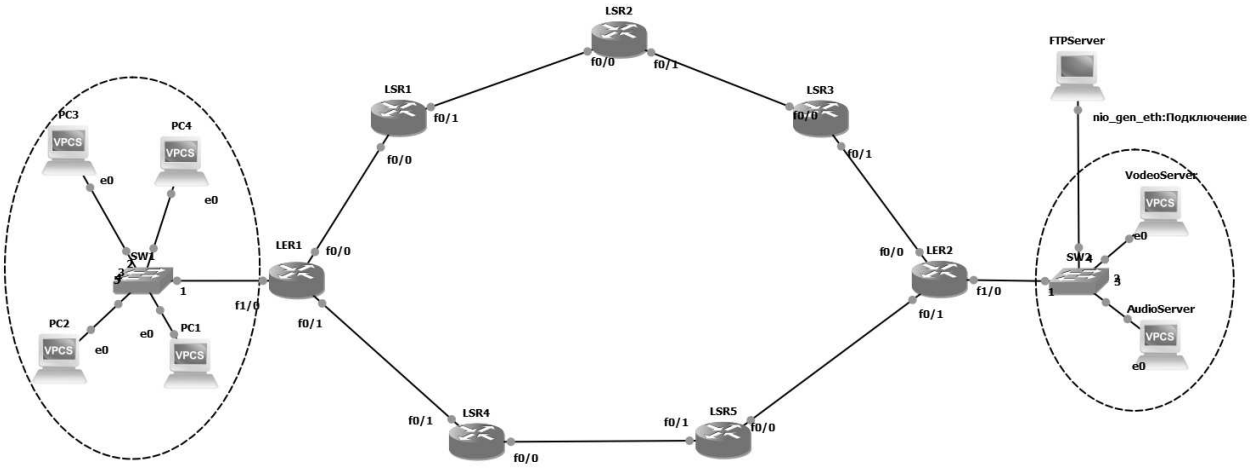


Рис. 1 Топология моделируемой сети.

Моделирование состоят из двух сценариев на представленных топологиях сети. Сценарий 1 на основе IP: сеть без TE (в составе протокола OSPF). Сценарий 2: на основе MPLS сети с TE.

В результате были сравнены метрики: время прохождения пакетов от одного конца линии связи к другому в сети MPLS TE и сети стандартной IP-модели. Для данного параметра, MPLS TE показало лучший вариант, чем традиционные сети IP[3,4].

В сценарии 1 все маршрутизаторы настроены, как обычные IP-маршрутизаторы и пакеты передаются при помощи протокола OSPF. В Сценарии 2 MPLS TE реализуется путем создания LSPs, и определение того, что трафик назначается соответствующим LSP. Перед тем как LSPs настроены, статус MPLS на интерфейсах, работающих с протоколом OSPF основных маршрутизаторов, устанавливается для включения. Пограничные маршрутизаторы, LER1 и LER2 рассматриваются в качестве источника и назначения LSP соответственно. Время отклика при передаче FTP пакетов в сети на базе MPLS TE была значительно ниже, чем в сети IP, как на рис. 2, а

также среднее время принятого пакета в MPLS TE лучше, чем в модели сети IP (см. рис. 3).

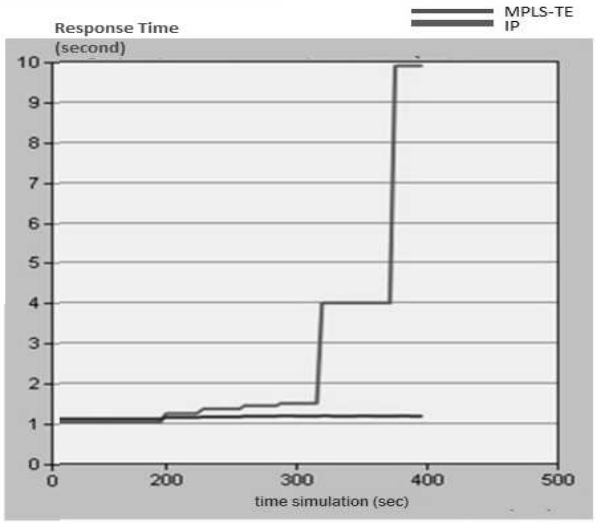


Рис.2 Среднее время приема пакета (пакет/сек).

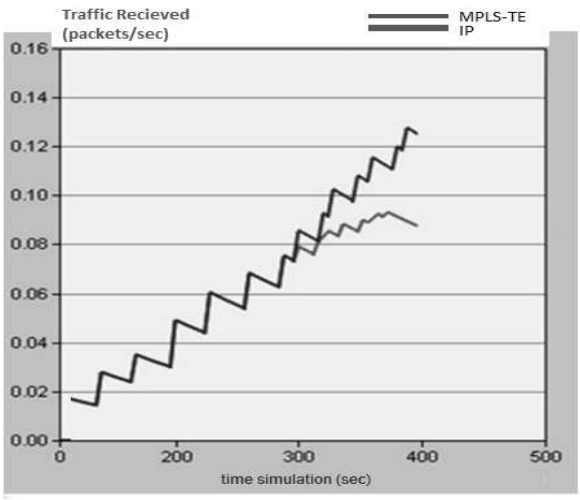


Рис.3 Время отклика пакета (сек).

На основе результатов моделирования можно сделать вывод о том, что MPLS обеспечивает лучшее решение в реализации таких приложений по сравнению с обычными IP-сетями. Кроме того, эта статья объясняет плохое использование линии связи в обычных IP-сетях. Видно, что сеть, которая сконфигурирована используя протокол маршрутизации OSPF, не способны эффективно обрабатывать входящий трафик. При увеличении сетевого трафика, кратчайший путь от исходного узла к узлу назначения сильно перегружается и приводит к потере данных передачи.

Было смоделировано и показано, что MPLS TE способен обрабатывать входящий трафик эффективней чем традиционные IP-сети, за счет распределения трафика по нескольким LSP, в соответствии с FEC, который не в состоянии достичь в обычном протоколе маршрутизации. Производительность сети значительно повышается при использовании MPLS TE на сети. Для внедрения данной технологии на сетях, необходимо значительное упрощение архитектуры сети.

Литература

1. Jasmina Barakovic Himzo Bajric, and Amir Husic., “Multimedia Traffic Analysis of MPLS and non-MPLS Network”, International Symposium ELMAR-2006, Zadar, Croatia, June 2012.
2. Najib Naja, “An Enhanced MPLS-TE for Transferring Multimedia packets”, International Journal of Advanced Computer Science and Applications, (IJACSA), Vol. 3, No.8, 2012.
3. Driss EI Ouadghiri, “Improving Quality of Service (QoS) in Multi-Protocol Label Switching Module”, IEEE Mediterranean Microwave Symposium, Nov 2013.
4. Tatiana Onali, “Quality of Service Technologies for Multimedia Applications in Next Generation Networks”, Ph.D. thesis, University of Cagliari, Italy, 2009.

УДК 621.3

ЦЕНТРЫ ОБРАБОТКИ ДАННЫХ НА БАЗЕ ТЕХНОЛОГИИ SDN

Роговой В. П.
Институт телекоммуникационных систем НТУУ «КПИ», Украина
E-mail: ihawk777@gmail.com

Data centers based on SDN technology

The Software-Defined Networking (SDN) technology as a solution of the problems of modern data centers. The essence and description of this technology are presented in this paper. Also the usage scenarios of the SDN are described for its clearness.

Центр обработки данных (ЦОД) является постоянно меняющейся системой, состоящей из тысяч программных компонент и инфраструктурных составляющих с гетерогенными компонентами и связями между ними. Реализация ЦОД может состоять из нескольких локаций разнесенных географически. Управление таким ЦОД, в реальном режиме времени, является технически сложной задачей связанной с наличием большого числа независимых компонент.

Постоянное увеличение трафика, вызванное ростом мобильного доступа, спросом на видеосервисы, использованием облачных вычислений приводит к тому, что современные дата-центры должны комплексно менять свою ресурсную базу. Дата-центры должны иметь возможность обрабатывать нестационарный объем трафика и совершать большой объем параллельных транзакций, уметь глубоко анализировать поступающие данные, быть легко перестраиваемыми под изменяющиеся запросы. При условии ограниченности ресурсов, ЦОД не могут бесконечно разрастаться.

Описание технологии. Решение многих вышеназванных проблем было найдено в виртуализации, а именно использовании технологии программно-определяемых сетей (SDN – Software-Defined Networking). Суть этой технологии заключается в отделении уровня управления сетью от уровня передачи данных. При этом все функции управления сетью (уровни администрирования устройств и управления трафиком) переносятся на отдельное устройство - контроллер. Таким образом, происходит централизация управления ресурсами сети, а именно более эффективное использование ресурсов и собственно автоматизация управления этой сетью. При этом сетевые элементы, у которых отобрали функции управления сетью, выполняют исключительно базовые задания – работают по продвижению пакетов. А распределение ресурсов сетевого элемента, то есть взаимодействие вышеназванного контроллера и коммутаторов, происходит благодаря специальным протоколам – например, OpenFlow. Для этого контроллер должен уметь взаимодействовать с приложениями, которые могут управлять сетью в режиме реального времени. Это дает возможность быстро изменять сеть под текущие нужды – например, перенаправлять трафик или выделять более широкую полосу пропускания во время HD

видеосвязи.

Функционирование в соответствии с данными принципами позволяет оптимизировать сетевую производительность, балансировку нагрузки и обеспечивает распределенную сетевую политику безопасности.

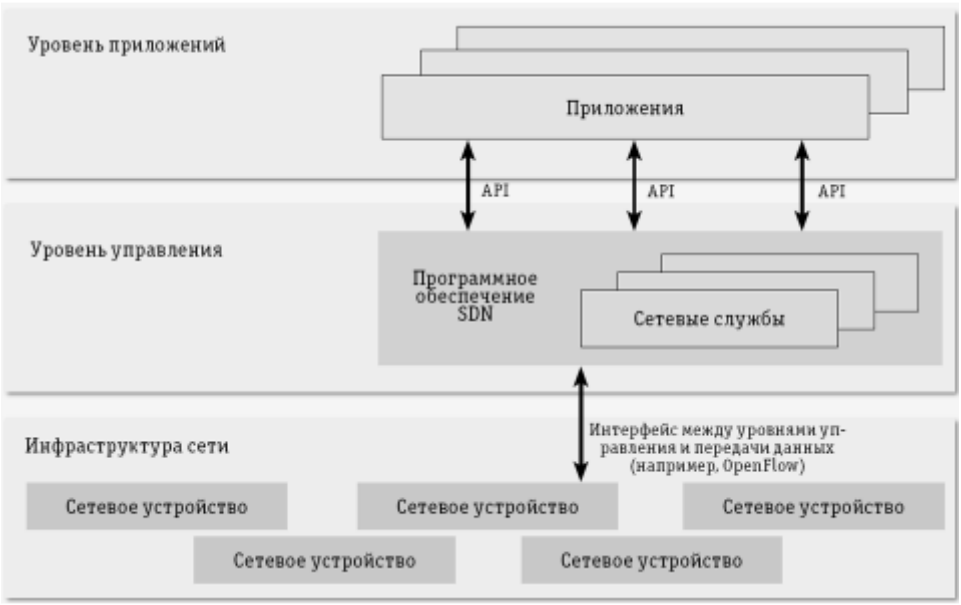


Рис.1 Структура технологии SDN.

Использование технологии. В настоящий момент на рынке присутствуют продукты от таких производителей как VMware, HP, Citrix, рассмотрим сценарии использования данных продуктов в IT среде, позволяющие раскрыть смысл данных технологий.

Сценарий 1-ый. Оптимальное распределение трафика между серверами в рамках ЦОД представляется довольно сложной задачей, связанной с различным уровнем нагрузки на элементы сетевой инфраструктуры. Также сложность представляет настройка протокола STP с точки зрения потребления ресурсов, а именно полосы пропускания в сетевой инфраструктуре.

Одним из решений данной ситуации является использование контроллера в качестве системы построения маршрутов (исключается участие протокола STP). Таким образом, использование данного решения полностью даёт возможность использовать полосу пропускания для трафика между различными широковещательными доменами без необходимости маршрутизации на маршрутизаторах.

На рис. 2 показано функционирование различных маршрутов уровня L2. Контроллер позволяет сформировать маршруты для потоков данных, избегая при этом появления петель.

Сценарий 2-ой. SDN позволяет сформировать единую наложенную сеть для множества дата-центров используя соединения на канальном уровне (без уровня маршрутизации L3). Используя данную возможность архитекторы приложений могут разнести компьютерные кластеры и точки их использования, что позволяет производить эффективное восстановление при

отказах.

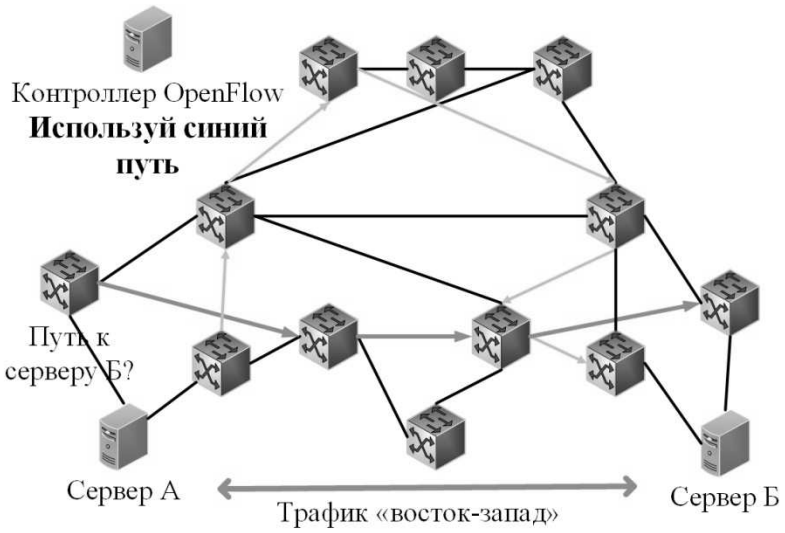


Рис.2 Первый сценарий использования технологии SDN

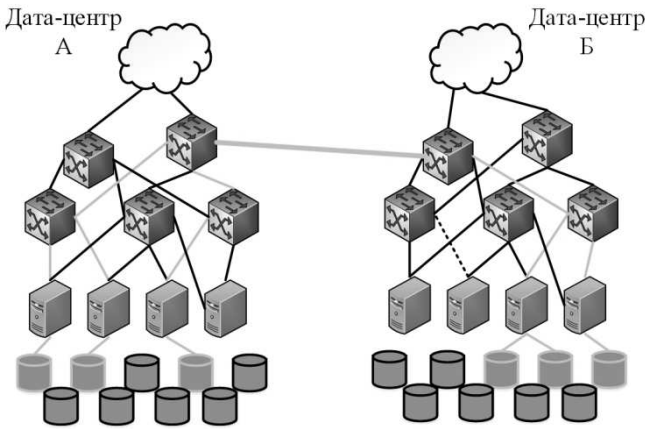


Рис.3 Второй сценарий использования технологии SDN

Выводы. Исходя из показанных сценариев видно, что технология позволяет обеспечить эффективное управление ресурсами ЦОД, а также обеспечить взаимодействие территориально-распределённых ЦОД для решения единых задач и обеспечивая при этом необходимую надежность и живучесть. Примерами внедрения данной технологии являются компании Google и Amazon, которые используют SDN в своей IT-инфраструктуре. Следует отметить, что следующим шагом развития данной технологии будет создание виртуализации вычислений и хранения данных, что позволит создавать распределённые системы с заданной надёжностью, масштабируемостью и защитой конфиденциальной информации.

Литература

1. Ying Cheng OPEN DATA CENTER ALLIANCE Master USAGE MODEL: Software-Defined Networking Rev. 2.0 (Электронный ресурс) / Ying Cheng, Vishy Ganti, Vince Lubsey [et al.] // OPEN DATA CENTER ALLIANCE – 2013-2014. – P. 16-17. – Режим доступа:http://opendatacenteralliance.org/docs/software_defined_networking_master_usage_model_rev2.pdf.

УДК 621.382

ПРОГРАММНАЯ IP АТС: ПРЕИМУЩЕСТВА И НЕДОСТАТКИ

Мишко М. С., Авдеенко Г.Л.
Институт телекоммуникационных систем НТУУ «КПИ», Украина
E-mail: muxas.93@mail.ru

Software-based PBX phone system solution: advantages and disadvantages

Analysis of the causes of the introduction of ip telephony. Advantages and disadvantages of IP PBX are presented.

Офисная АТС была и остается одним из важнейших инструментов общения сотрудников бизнес-организаций с компаниями-партнерами, поставщиками материалов и комплектующих, дистрибьюторами и т.д. Основу ее функциональности изначально составляет решение задач соединения телефонных аппаратов вызывающего и вызываемого абонентов, поддержания сеанса связи и разрыва соединения по завершению разговора. К этим «трем китам» коммутации линий голосовой связи постепенно добавлялись все новые и новые функции и сервисы, и в настоящее время их количество достигает двух-трех десятков (в зависимости от модели АТС).

Современные мини-АТС включают в себя множество различных услуг, однако для компаний, только начинающих свой бизнес, цена создания на их базе внутренней телефонной сети иногда кажется «неподъемной». И в поисках более дешевого (но равнозначного по функциональности) технического решения стартапы идут в сегмент компьютерной, то есть VoIP телефонии, предоставляющей возможность передачи в одном канале голосовой и цифровой информации (а локальная компьютерная сеть «по умолчанию» в компании уже есть). [1]

На рынке VoIP телефонии представлен ряд учрежденческих телефонных станций, работа которых основана на протоколе IP (Internet Protocol), предназначенном для организации обмена данными в цифровом виде (в том числе, речи) с помощью пакетной коммутации. Такие станции образуют класс IP-АТС, с входящими в него двумя группами: 1) аппаратные IP АТС и 2) программные IP АТС, в основной массе представляющие собой Linux-дистрибутивы или исполняющие файлы под ОС Windows.

В программной IP АТС все функции аналоговых, цифровых и гибридных телефонных станций, выполняемые коммутаторами, маршрутизаторами и другим приборным оборудованием, эмулируются специальным ПО, которое устанавливается на любом работающем в компании сервере или десктопе. [2]

Во второй группе класса IP-АТС обосновались сегодня около 20 разновидностей так называемого «свободного ПО» с открытым исходным кодом, по определению, предоставляющего потребителям право дополнять его новыми функциями, в которых возникла необходимость. При этом почти половина ареала свободного ПО для программных АТС относится к

бесплатным продуктам. А среди них безусловным лидером является программная IP-АТС Asterisk, далеко оторвавшаяся от конкурентов, которые делят между собой оставленные ею аутсайдерам примерно 15% рынка IP-АТС с открытым кодом. И на ее использование ориентируется большинство «стартующих» компаний малого бизнеса. [3]

Достоинства программных IP АТС.

Основные достоинства программных IP-АТС (на примере IP-АТС Asterisk) можно свести к следующему**:**

- полный набор базовых и дополнительных функций мини АТС.
- поддержка работы со Skype;
- обеспечение видеосвязи;
- возможности IP-АТС могут быть расширены, например, в части параллельного обслуживания десятков и даже сотен телефонных разговоров, если к серверу с установленным ПО Asterisk подключить компьютерные платы, обеспечивающие связь с линиями высокой пропускной способностью типа T1/E1.

Конкурирующие же бесплатные программы, предназначенные в основном для IP-АТС специфических применений, не обладают такой совокупностью характеристик (хотя в своих областях по отдельным показателям могут превосходить Asterisk).

Администрирование Asterisk может осуществляться несколькими графическими средствами управления, но выбор большинства пользователей, как правило, останавливается на веб-интерфейсе FreePBX, с помощью которого без особой сложности добавляются или заменяются абонентские номера и функции.

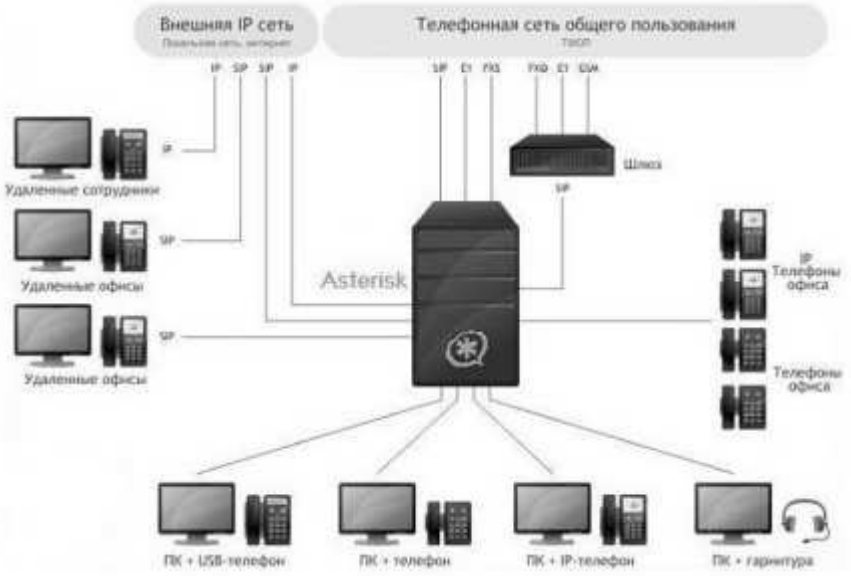


Рис. 1 Пример построения телефонной сети на базе программной IP АТС Asterisk.

К программной IP АТС Asterisk могут быть подключены как программные телефоны (софтфоны), так и все разновидности аппаратных

пользовательских IP телефонов (с интерфейсами IP, USB, Wi-Fi) (рис.1).

Недостатки программных IP АТС.

Недостатки применения программных IP АТС заключаются в финансовых издержках и рисках связанных со слабой защитой от возможного несанкционированного доступа к ресурсам АТС, а именно:

- Расходы на инсталляцию Aterisk на сервере. Поскольку это сложное ПО, использующее в качестве платформы операционную систему Linux, необходим специалист, хорошо разбирающийся в ней. То есть для установки Asterisk придется привлечь компанию-интегратора [4].
- Расходы на администрирование и обслуживание. Для выполнения этих функций требуется профессионал в области работы с Linux, знающий Asterisk, а также технологии и оборудование IP-телефонии. Такого «дорогого сотрудника» придется принять в штат компании или «вырастить» в своих рядах, потратившись на его обучение, а затем выплачивая ему высокую зарплату.Таким образом, стоимость владения и эксплуатационного сопровождения бесплатной программной АТС с течением времени может превысить затраты на приобретение аппаратной IP-АТС с аутсорсинговой службой поддержки.
- Легко реализуемая возможность внешнего вторжения в АТС. Самая частая причина взломов Asterisk – неумение правильно сделать базовые настройки безопасности программной IP АТС. Вторая слабость защиты обусловлена тем, что как отмечалось выше, в Asterisk «свободными программистами» часто внедряются новые функциональные модули (что, собственно, могут делать и сами пользователи), которые привносят в базовое ПО новые уязвимости. Найти эти бреши опытным хакерам не представляет труда и в результате успешной атаки через Asterisk прокатывается вал транзитных звонков, за которые придется заплатить кругленькую сумму.

Рассмотрены существующие тенденции, представленных на рынке телефонии, решений для бизнеса. Представлены преимущества и недостатки программных IP АТС. При выборе того или иного решения, обеспечивающего потребность коммуникации сотрудников бизнес-организаций, необходимо учитывать полученный выигрыш и возможные риски.

Литература

1. http://it-center.kiev.ua/stati/49.html.
2. Гольдштейн Б.С., Пинчук А.В., Суховицкий А.Л., М.: Радио и связь, 2006. - 336 с.: ил. ISBN 5-256-01585-0.
3. http://www.asterisk.org/.
4. http://www.skomplekt.com/solution/programmnaya_ip_ats.htm.

УДК 621.3

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ГАРАНТИРОВАННОГО ПРЕДОСТАВЛЕНИЯ СЕРВИСОВ В ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Галенко Е.В., Лисковский И.О.
Институт телекоммуникационных систем НТУУ «КПИ», Украина
E-mail: zhenyagalonko@gmail.com

Problems of providing guaranteed representation of services in the telecommunications network

In this paper analysis, the main problems associated with the provision quality of services of telecom operators and factors that make difficult to control the quality of modern communication networks.

Сегодня происходит серьезное изменение структуры и характера информации, передаваемой в телекоммуникационных сетях как корпоративного уровня, так и уровня операторов связи. Главным поставщиком данных становится Интернет, сервисы которого пользуются все возрастающим спросом. Меняются подходы к построению сетей, и на первый план выходят сети следующего поколения, то есть сети NGN (Next Generation Network)/FGN(Future Generation Network). При этом никаких количественных ограничений на типы и характеристики трафика, которые реализуются в сети не накладываются. Такая постановка задачи приводит к необходимости выработки новых механизмов и модернизации уже имеющихся механизмов поддержания заданного качества при оптимальном использовании ресурсов провайдера(ISP). Также сложность заключается в том, что большинство провайдеров имеют у себя внутри инфраструктуру формирования собственных сервисов, а также, должны предоставить выделенные ресурсы для транзита сервисов через собственную инфраструктуру с обеспечением заданного качества и систем оценки и контроля за реальным качеством предоставленной услуги.

Основные проблемы, связанные с обеспечением качества услуг связи, с которыми сталкиваются операторы[1]:

1. Совместное использование ресурсов сетей, использующих принципы коммутации каналов (КК) и коммутации пакетов (КП) КК и КП, а также ресурсов сетей фиксированной и мобильной связи за один сеанс связи при предоставлении новых услуг.

2. Снижение общего коэффициента надежности сети при предоставлении инфокоммуникационных услуг из-за использования большого количества разнотипных программных и аппаратных средств (маршрутизаторы, шлюзы, контролеры шлюзов, серверы и т.д.) разных производителей.

3. Рост полосы пропускания, доступной каждому абоненту, происходит по закону Нильсена (Jakob Nielsen), согласно которому средняя полоса пропускания, доступная абоненту при развитии технологий доступа, увеличивается на 50 % ежегодно. Такой рост приводит к увеличению потребляемого трафика и, как следствие, не способности транспортной сети

обеспечить требуемое качество услуг связи без использования механизмов управления ресурсами транспортной сети.

Таблица 1. Количество подключений в мире [2]

Количество активных подключений от общего числа IP-подключений, %	**2015**	**Прогноз на 2019**
Количество подключений IPv6, в том числе мобильных	16	47
Подключение к IP-сетям, фиксированные линии связи	56	39
Подключение к IP-сетям, Wi-Fi	41	49
Подключение к IP-сетям, мобильные сети связи	3	12
Трафик сетей метро	49	62
Количество подключений с ПК	82	48
Количество TV-подключений	6	8
Интернет-видео, корпоративное и пользовательское	57	75
Internet-Video-to-TV	11	14
Трафик домашних и муниципальных сетей	57	63
Количество модулей M2M	3	2,8
Скорость подключения свыше 50 Мбит/с	12	22

Из таблицы видно, что количество подключений в мире увеличивается с каждым годом. Самый большой рост наблюдается в мобильных сетях связи, который на 2019 год вырастет в 4 раза, чего нельзя сказать о подключениях с ПК. Это объясняется тем, что в современном мире в связи с развитием мобильных приложений, количество пользователей ПК уменьшается.

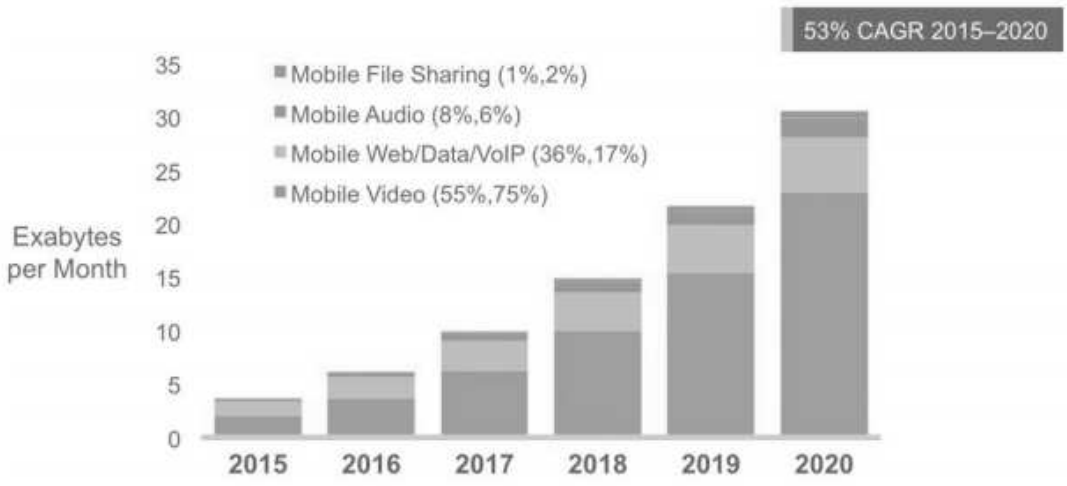


Рис. 1 Прогноз роста трафика мобильных мультимедийных приложений[3].

С учетом тенденции постоянного расширения числа приложений с различными требованиями к характеристикам качества обслуживания и более активного использования smart-устройств, а также появление новых видов услуг, создающих нагрузки с низкой предсказуемостью требуют разработки новых механизмов обеспечения QoS.

Активное использование в качестве доступа беспроводных сетей требует анализа и разработки механизмов сопряжения множеств показателей качества при выгрузке трафика из сети доступа в транспортную сеть.

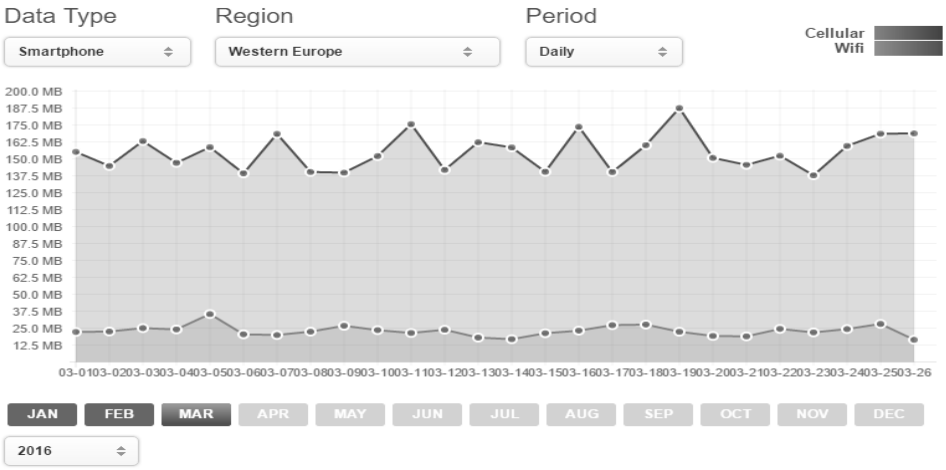


Рис. 2 Статистика по потреблению данных сотовый связью и Wi-Fi с помощью смартфона за 3 месяца 2016 года[4].

Факторы, которые затрудняют управлением качеством в современных сетях связи:

1. Особенности восприятия пользователем мультимедийной информации и различие пользователей по классам обслуживания;
2. Независимое развитие уровней: не всегда на уровне услуг можно учесть влияние факторов физической среды и инфраструктуры,
3. Процедуры совместимости отдельных сетей и/или сегментов сети;
4. Появление новых видов трафика и новых требований к услугам;
5. Использование операторами традиционных механизмов QoS и политик обеспечения качества;
6. Создание непредсказуемых нагрузок на сеть приложениями операторов услуг и OTT;
7. Мобильность пользователя: смена сетей доступа, географическое перемещение;
8. Компьютеризация телекоммуникационных устройств и их подверженность угрозам (вопросы информационной безопасности);
9. Отсутствие механизмов обратной связи и независимой оценки качества на стороне пользователя [5].

Литература

1. Шалагинов В.А. Сравнительный анализ архитектур для обеспечения качества услуг связи в сетях следующего поколения // спецвыпуск TComm. - 2009
2. VNI Mobile Forecast Highlights, 2015-2020 [Электронний ресурс] – Режим доступа: http://www.cisco.com/assets/sol/sp/vni/forecast_highlights_mobile/index.html
3. Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020 [Электронний ресурс] – Режим доступа: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html
4. Cisco Data Meter [Электронний ресурс] – Режим доступа: http://www.cisco.com/c/dam/m/en_us/solutions/service-provider/vni-forecast-widget/data-meter/index.html
5. Симонина О.А. Задачи управления качеством услуг в условиях перехода к сетям post-NGN [Электронний ресурс] – Режим доступа: https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Documents/Events/2014/09_Astana/Session_1_Simonina_2.pdf

УДК 621.3

ЗАСТОСУВАННЯ ПРОГАМНО-ВИЗНАЧУВАНИХ МЕРЕЖ (SDN) В ТЕХНОЛОГІЇ 5G

Марціленко С.В., Глоба Л.С.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: martsel3@gmail.com

USING SOFTWARE DEFINED NETWORKS (SDN) IN 5G TECHNOLOGY

In this paper Software Defined Networks is examined according to the requirements that are applied for the construction of new communications networks. Features of realization SDN for supporting 5G technology are defined. Logical structure of SDN is reviewed.

У сучасному світі до сфери інформаційних технологій висувають все більше вимог, що стосується побудови нових мереж, існує ряд проблем, які виникають при цьому.

Мережі, що створюються мають підлаштовуватися під такі умови, як:

- зростання обсягів трафіку і модифікація його структури;
- потреба підтримки мобільних користувачів і соціальних мереж;
- реалізація cloud-сервісів [1].

Технологія 5G – така технологія, яка забезпечить доступ до даних скрізь, у будь-який час та на великій швидкості, тобто покращить якість обслуговування(QoS).

Очікують, що розширена інфраструктура п’ятого покоління(5G) стане "нервовою системою" у цифровому суспільстві та економіці. Ключові показники (5G) розраховують за умовою того, що вони мають бути гнучкими, масштабованими та надійними. Це можна реалізувати, завдяки впровадженню програмно-визначуваних мереж (software-defined networking, SDN).

SDN мають вирішити існуючі проблеми розвитку інформаційно-комунікаційних мереж, забезпечити єдиний доступ до їхніх ресурсів і стати основою технології 5G.

У традиційній моделі мережеві провайдери змушені планувати кількість портів, комутаторів і маршрутизаторів з великим запасом, щоб покривати можливе різке зростання трафіку. До того ж, оновлення програмного забезпечення і апаратних засобів іноді може викликати необхідність у придбанні додаткового обладнання та залучення додаткових спеціалістів, які займаються підтримкою додаткового мережного обладнання та програмного забезпечення, що функціонує в IT-середовищі. Це, в свою

чергу, вимагає додаткових витрат та зумовлює затримки в оновленні інфраструктури.

Таким чином, вивчення шляхів організації архітектури SDN –мереж є актуальним завданням.

Розглянемо детальніше технологію SDN. Програмно-визначувана мережа – така система для передавання даних, у якій керування мережею реалізується програмно. Оскільки процес маршрутизації в SDN-мережі виконується програмним забезпеченням, то в ній, в першу чергу, віртуалізуються пристрої комутації та маршрутизації. Структура звичайного мережного пристрою (рис.1), наприклад, комутатора або маршрутизатора складається із таких компонентів:

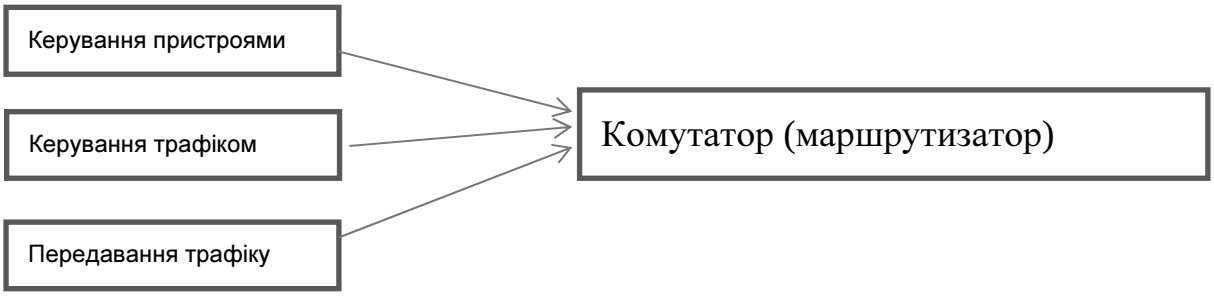


Рис. 1. Структура комутатора(маршрутизатор).

Основним напрямком підвищення ефективності функціонування SDN-мережі є застосування динамічного розподілу ресурсів мережі, створивши специфічну фізичну мережну інфраструктуру, здатну підтримувати набагато ширший спектр вимог з можливістю створення виділених мереж, які можуть бути контрольовані користувачами, наприклад, через корпоративні портали самообслуговування. Ключовим елементом такого рішення є можливість гнучко адаптувати інфраструктуру до різних вимог прикладного характеру. Для цього потрібно сформувати логічну структуру програмно-визначуваної мережі. Щоб це зробити, необхідно реалізувати керування системою програмно та відокремити його від самих пристроїв. Таким чином, отримаємо логічну структуру SDN-мережі (рис.2) [1-2].

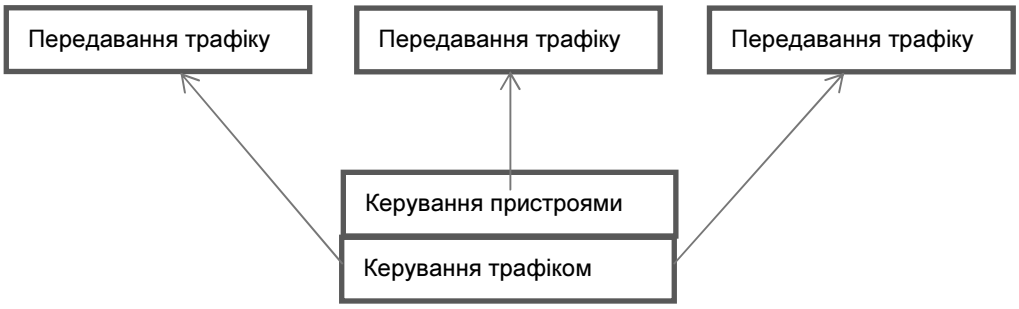


Рис. 2. Логічна структура програмно-визначуваної мережі.

Побудова такої моделі забезпечує отримання відкритого інтерфейсу між відокремленими елементами керування та функціями передачі трафіку, спрощеного керування мережею, побудови та обслуговування з меншими витратами, а також віртуалізації пристроїв комутації та маршрутизації. Для забезпечення відкритого інтерфейсу застосовують протокол OpenFlow. OpenFlow – це протокол керування процесом обробки даних, які передаються мережею передавання маршрутизаторами або комутаторами. Протокол реалізує технологію SDN, дозволяє використовувати у складі програмно-визначуваної мережі устаткування різних виробників [3].

Мережна індустрія зазнає значні зміни, викликані появою програмно-визначуваних мереж, віртуалізації мережевих функцій (network-functions virtualization, NFV) та інших технологій віртуалізації, які мають зробити мережі більш гнучкими, динамічними, масштабованими і доступними, але виникає недолік: процес обробки трафіку відбувається повільніше. Надання мережі у вигляді сервісу забезпечує більш швидку реакцію мережної інфраструктури на запити споживачів під впливом підвищення інтенсивності використання мобільних технологій, збільшення обсягів передачі даних завдяки технологіям Інтернет речей (IoT), стратегії BYOD і cloud-сервісам [4].

Таким чином, для створення мережі 5G актуально застосовувати програмно-визначувані мережі (Software Defined Networks), які мають певні переваги, такі як: гнучкість, доступність, масштабованість, а також дозволяють реалізувати процес маршрутизації або комутації програмно.

Література

1. Мережеві технології SDN - Software Defined Networking. [Електронний ресурс]. Режим доступу до ресурсу: http://it-ua.info/news/2015/03/12/merezhev-tehnolog-sdn-software-defined-networking.html.
2. David Soldani, Bernard Barani, Rahim Tafazolli, Antonio Manzalini, Chih-Lin I. SOFTWARE DEFINED 5G NETWORKS FOR ANYTHING AS A SERVICE. “IEEE Communications Magazine” – C.72-73.
3. Y.Qi, M.Z. Shakir, K.A. Qaraqe, M.A. Imran. Emerging Features of 5G. "Asurveyon 5G architectures: IoT driven applications, Interference management and emerging features" – C.132
4. Сеть по запросу. [Електронний ресурс]. Режим доступу до ресурсу: http://www.pcweek.ua/themes/detail.php?ID=151511.

УДК 621.396.43

ДОСЛІДЖЕННЯ ПЕРЕДАВАННЯ РАДІОСИГНАЛУ ЦИФРОВОГО ТЕЛЕБАЧЕННЯ СТАНДАРТУ DVB-S З ВИКОРИСТАННЯМ РАДІОКАНАЛУ ТЕРАГЕРЦОВОГО ДІАПАЗОНУ

Наритник Т.Н., Набока Б.Ю., Авдєєнко Г.Л.
НДІ телекомунікацій НТУУ «КПІ»
Email: iec@nbi.com.ua

Digital TV of DVB-S standard radio signal research transmission in terahertz radio channels

The results of mathematical modeling and simulation of radio relay lines in terahertz range, as well as studies of physical models of digital satellite TV signal of DVB-S standard transmission using terahertz range are shown. The results allow to draw conclusions about the ability of usage of radio relay lines in high-rate telecommunications networks.

Один з перспективних напрямів розвитку сучасних телекомунікацій, напівпровідникової техніки і радіоелектроніки пов'язаний з освоєнням так званої «терагерцової щілини» - області електромагнітного спектру, що лежить приблизно в діапазоні від 100 до 3000 ГГц [1–5].

Терагерцові і субтерагерцові частоти вже кілька років розглядаються як способи реалізації швидкодіючих комунікаційних каналів, призначених для використання у місцях розташування, де прокладка волоконно-оптичного кабелю утруднена або неможлива. На сьогоднішній день цей діапазон практично не застосовується для комунікації, що пов'язано з відсутністю до недавнього часу реально функціонуючих радіоканалів терагерцового діапазону. Певні перспективи можуть надати створені радіоканали передачі даних в терагерцовому діапазоні з пропускною здатністю більше 1 Гбіт/с [4–5] і побудовані на їх основі радіорелейні системи для безпроводової передачі телевізійних програм високої та надвисокої чіткості, які потребують цифрових каналів з пропускною здатністю до 6 ГБіт/с.

В зв’язку з наведеним вважається доцільним проведення математичного та імітаційного моделювання радіорелейної лінії терагерцового діапазону, а також дослідження фізичної моделі передавання радіосигналу цифрового супутникового телебачення стандарту DVB-S з використанням макету радіоканалу терагерцового діапазону. Параметрами, що досліджуються є: відстань між радіорелейними станціями, відношення сигнал/шум SNR та ймовірність бітових помилок BER.

Вхідні дані для розрахунку дальності дії макету радіоканалу терагерцового діапазону (рис. 1) наведено у табл.1, виходячи з яких було знайдено можливі відстані (табл.2) за ідеального випадку поширення

радіохвиль (враховувалось лише затухання вільного простору), без дощу (додатково враховуючи втрати в атмосфері) та в дощі.

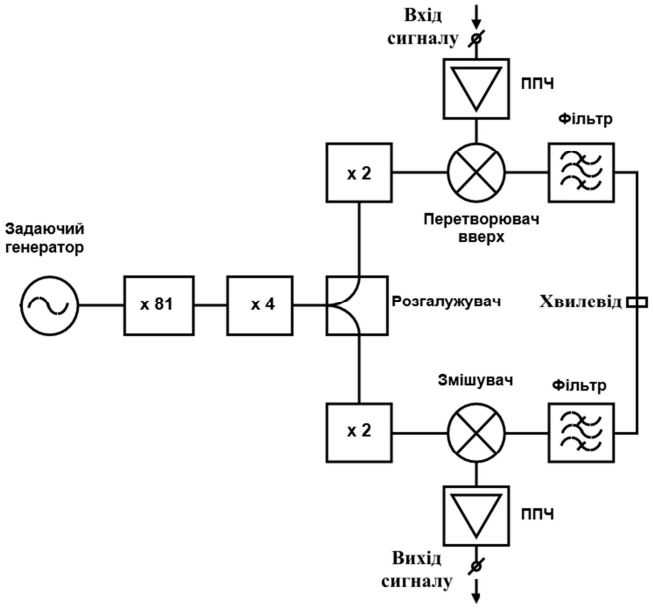


Рис.1 Схема макету радіоканалу терагерцового діапазону.

Таблиця 1. Вхідні дані розрахунку радіолінії.

Частота передача f, ГГц	Інтенсивність дощу $\gamma_д$, мм/год	Температура середовища T_0, К	Потужність передавача без ПП $P_{пер}$, мкВт	Потужність передавача $P_{пер}$, мВт	Діаметр прд. та прм. антен D, $м$	Коефіцієнт використання поверхні антени η, рази	Ширина спектру частот Δf, МГц	Коефіцієнт шуму приймача, рази
131.2	35	290	50	50	0,3	0,6	440	18,241

Таблиця 2. Результати розрахунку відстані зв'язку.

Погодні умови	При потужності підсилювача $50 \cdot 10^{-6}$, Вт			При потужності підсилювача $50 \cdot 10^{-3}$, Вт		
	Постійна С, дБ	Сумарні ослаблення	Відстань, км	Постійна С, дБ	Сумарні ослаблення	Відстань, км
Ідеалізований випадок	146,333	146,334	3,773	176,333	176,328	119,229
Без дощу	146,333	146,331	2,817	176,333	176,324	18,165
В дощі	146,333	146,492	0,831	176,333	175,162	2.306

Для підтвердження можливості передачі інформації на дані відстані і дослідження характеристик сигналу було проведено імітаційне моделювання радіорелейної лінії терагерцового діапазону у програмному середовищі Visual System Simulator. Параметрами, що досліджуватись, були зміни рівнів сигналу між передавачем та приймачем (рис.2), спектральних характеристик одного каналу на вході і виході моделі (рис. 3-4) та сигнальні сузір'я на вході і виході імітаційної моделі (рис. 5-6).

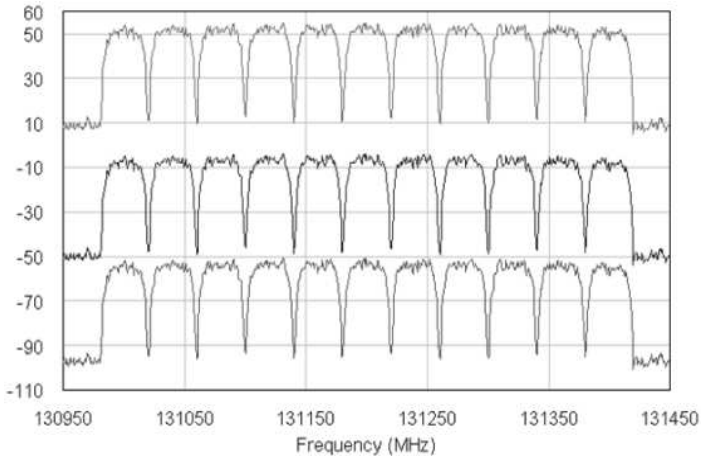


Рис. 2 Зображення сигналу до (синім кольором) і після (рожевим кольором) підсилення передавальної антени та на виході приймальної антени (червоним кольором).

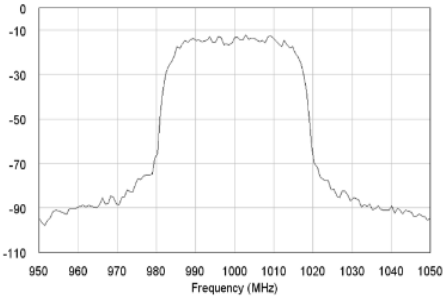


Рис. 3 Спектр сигналу DVB-S на вході приймача.

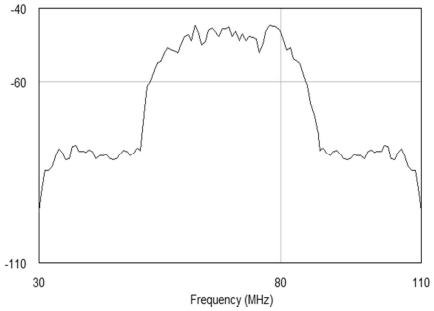


Рис.4 Спектр сигналу DVB-S на виході приймача.

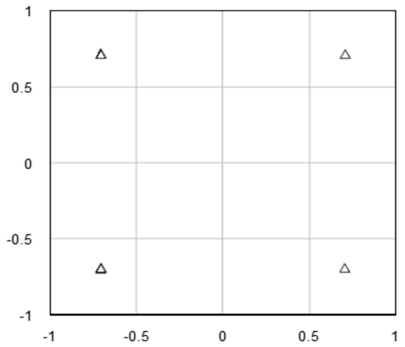


Рис.5 Констеляційна діаграма на вході приймача.

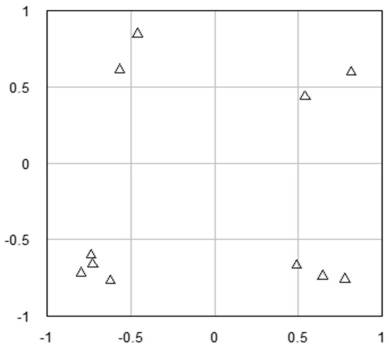


Рис. 6 Констеляційна діаграма на виході приймача.

При дослідженні фізичної моделі (макету) було виконано передавання сигналу стандарту DVB-S по радіоканалу терагерцового діапазону (рис. 7) з відповідними замірами (таблиця. 3, рис.8).

Таблиця 3. Результати експериментальних досліджень.

Місце заміру	Lev, dBm	MER, dB	N. MAR dB	EVM,%	aBER	bBER	Modulation	Vsymb, Msymb/s	Quality, %	FEC
Вх прд	-42	21.5	15	8.9	10^{-8}	10^{-6}	QPSK	27.500	100%	3/4
Вихпрм	-42	20	13	11,2	10^{-8}	10^{-6}	QPSK	27.500		3/4

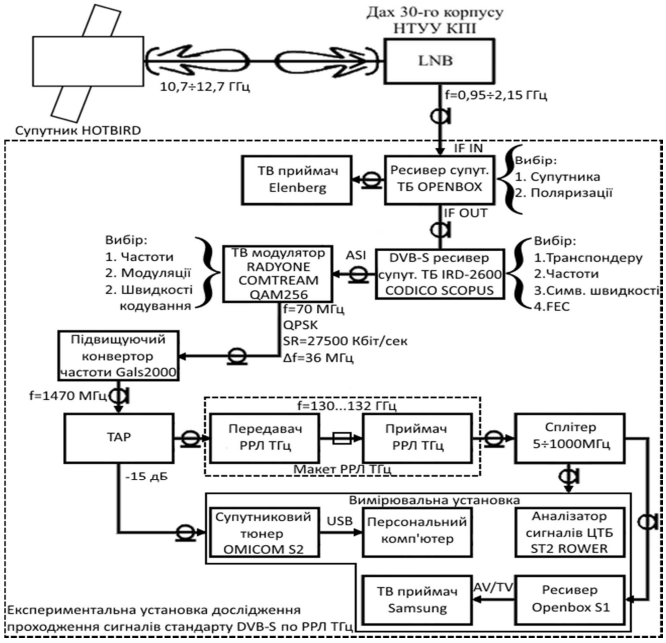


Рис. 7 Схема дослідження передавання сигналів DVB-S.

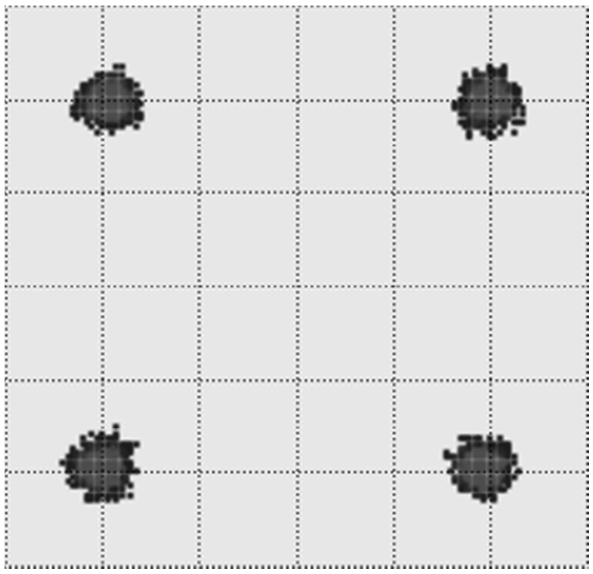


Рис. 8 Констеляційне сузір'я сигналу DVB-S на виході макету радіоканалу.

Проведені розрахунки вказують на те, що радіоканалом терагерцового діапазону є можливість передавати інформацію на відстані до 2 км при потужності підсилювача 50 мВт з високою якістю. Експериментальне дослідження підтвердило можливість передавання по радіоканалу терагерцового діапазону радіосигналу цифрового супутникового телебачення стандарту DVB-S з показниками BER на рівні 10^{-6} .

Література

1. Ільченко М. Ю. Передавальний та приймальний радіотракти радіорелейних систем терагерцового діапазону / Ільченко М. Е., Наритник Т. М., Радзіховський В. М., Кузьмін С. Е., Лутчак А. В. // Цифрові технології № 17. – 2015. – с. 17-29. – Режим доступу: http://www.mitris.com/files/16-29.pdf
2. Кравчук С.О. Телекомунікаційні системи терагерцового діапазону. Монографія.//Житомир.: ФОП «Євенок О.О.».--2014.-394с. Кравчук С.О., Наритник Т.М.
3. M.Ye. Ilchenko Transceiver for 130-134 GHZ band and digital radiorelay system. M.Ye. Ilchenko, T.N. Narytnik, S.Ye. Kuzmin, A.I. Fisun, O.I. Belous, V.N. Radzikhovsky// Telecommunications and Radio Engineering.- Volume 72.- Number 17.- 2013.-P.1623-1638.
4. Пат. 93139 Україна, МПК H04B 7/165 (2006.01). Канал передачі даних в терагерцовому діапазоні з пропускною здатністю більше 1 Гбіт/с / Ільченко М.Ю., Наритник Т.М., Казіміренко В.Я., Радзіховський В.В, Кузьмін С.Є.-Заявник і патентовласник Національний технічний університет «Київський політехнічний інститут».-.№u20140189, заявл. 25.02.2014; опубл. 25.09.2014, Бюл.№8.-5с: іл.
5. Narytnik T.N. Possibilities of Using THz-Band Radio Communication Channels for Super High-Rate Backhaul// Telecommunications and Radio Engineering, 73 (15):1361-1371 (2014).

УДК 621.396.43

ДОСЛІДЖЕННЯ ПЕРЕДАЧІ СИГНАЛІВ DVB-C ПО РАДІОРЕЛЕЙНІЙ ЛІНІЇ ТЕРАГЕРЦОВОГО ДІАПАЗОНУ

Наритник Т.Н., Набока Б.Ю., Авдєєнко Г.Л.
НДІ телекомунікацій НТУУ «КПІ»
E-mail: iec@nbi.com.ua

Research of DVB-C signals transmission over terahertz radio relay line

The results of DVB-C signals transmission over radio relay line are given in the thesis. The issue regarding the capabilities of physical model on the bottom part of its bandwidth is studied.

В роботі було проведено дослідження передачі групового сигналу цифрового телевізійного мовлення, що складається з одного, двох та трьох сигналів стандарту DVB-C, по радіорелейній лінії терагерцового діапазону (РРЛ терагерцового діапазону). Дослідження сигналів саме стандарту DVB-C було обрано тому, що у цьому стандарті є можливість використовувати різнопозиційні види модуляції (QAM-16,32,128,256).

Під час дослідження було проведено три експерименти :

1) передача по РРЛ терагерцового діапазону групового сигналу цифрового телевізійного мовлення, що складається з одного сигналу DVB-C на частоті 850 МГц, який переносить багатопрограмний транспортний потік на швидкості 41,25 Мбіт/с;

2) передача по РРЛ терагерцового діапазону групового сигналу цифрового телевізійного мовлення, що складається з двох сигналів DVB-C на частотах
850 МГц та 858 МГц із сумарною швидкістю транспортного потоку 82,5 Мбіт/с;

3) передача по РРЛ терагерцового діапазону групового сигналу цифрового телевізійного мовлення, що складається з трьох сигналів DVB-C на частотах
842 МГц, 850 МГц та 858 МГц із сумарною швидкістю транспортного потоку 121,75 Мбіт/с.

Експериментальна установка для дослідження проходження сигналів DVB-C по РРЛ терагерцового діапазону зображена на рис.1.

За допомогою двоканального трансмодулятора WISI OV75 та модулятора RADYNE COMSTREAM QAM-256 виконується перетворення вхідних сигналів стандарту DVB-S, що прийнято супутниковою антеною від супутника HOT BIRD (табл.1), в сигнали стандарту DVB-C. При цьому при формуванні сигналів DVB-C встановлюється необхідна модуляція (QAM-64, QAM-128, QAM-256), символьна швидкість (в залежності від модуляції та швидкості завадостійкого кодування), проміжна частота (842, 850 та 858 МГц) та ширина спектру (6 – 8 МГц в залежності від символьної швидкості).

Таблиця 1. Вхідні параметри сигналів цифрового телебачення стандарту DVB-S від супутника HOT BIRD (13° сх.д), що поступають на вхід формувачів сигналів DVB-C.

Номер каналу	***Вхідний сигнал, МГц***	***Проміжна частота, МГц***	***Символьна швидкість, Ксим/сек***	***Бітова швидкість, Мбіт/сек***	***Модуляція***	***FEC***		***Інформаційна швидкість, Мбіт/сек***	***Ширина спектру, МГц***
						Conv.	***R.S.***		
1	11179	1429	27500	55	QPSK	3/4	$\frac{188}{204}$	38,015	36
2	11137	1387	27500	55	QPSK	3/4	$\frac{188}{204}$	38,015	36
3	11334	1584	27500	55	QPSK	3/4	$\frac{188}{204}$	38,015	36

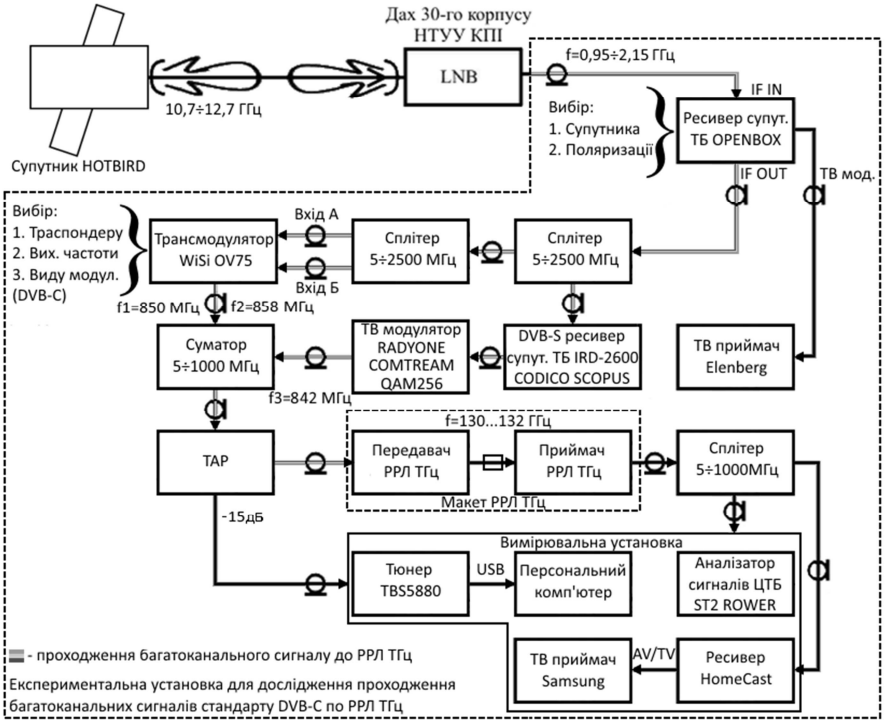


Рис. 1 Схема дослідження передачі сигналів стандарту DVB-C по РРЛ терагерцового діапазону

На вході та на виході макету РРЛ терагерцового діапазону виконується вимірювання наступних параметрів кожного сигналу DVB-C, що входить до складу групового сигналу телевізійного мовлення: а) рівень сигналу (LEV), відношення потужностей несівного коливання до шуму (C/N), запас завадостійкості (N.MAR), коефіцієнт нерівномірності спектру (FLAT), коефіцієнт бітової помилки (BER) за допомогою аналізатор спектру цифрового телебачення ST2 Rover; б) Quality за допомогою ресиверу цифрового кабельного телебачення Homecast; в) зображення констеляційних діаграм за допомогою тюнеру ефірного та кабельного цифрового телебачення Qbox TBS5880.

Як приклад, розглянемо заміри параметрів другого сигналу DVB-C (з несівною частотою 850 МГц) групового сигналу телевізійного мовлення за

найгіршого випадку (при модуляції QAM-256 і передачі трьох каналів сигналу DVB-C) на вході та виході макету РРЛ ТГц (табл.2, рис 3-4).

Таблиця 2. Характеристики другого каналу сигналу цифрового телебачення стандарту DVB-C при проходженні по радіорелейній лінії терагерцового діапазону на проміжній частоті 850 МГц.

Місце заміру	***Lev, dBm***	***C/N, dB***	***N. MAR dB***	***FLAT, dB***	***BER***	***Modulation***	***Vsymb, Msymb/s***	***Quality, %***
Вх прд	-29	36	10	3	10^{-8}	QAM-64	6,875	100
Вих прм	-40	33	8	1	10^{-8}	QAM-64	6,875	
Вх прд	-30	30	4	2	10^{-7}	QAM-128	5,892	67-100
Вих прм	-40	23	9	2	10^{-8}	QAM-128	5,892	
Вх прд	-23	>36	10	3	10^{-8}	QAM-256	5,156	33-58
Вих прм	-32	28	0	3	10^{-4}	QAM-256	5,156	

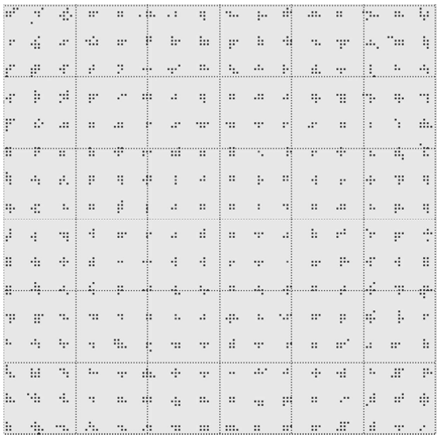


Рис. 3 Констеляційна діаграма сигналу з несною 850 МГц на вході макету при модуляції QAM-256.

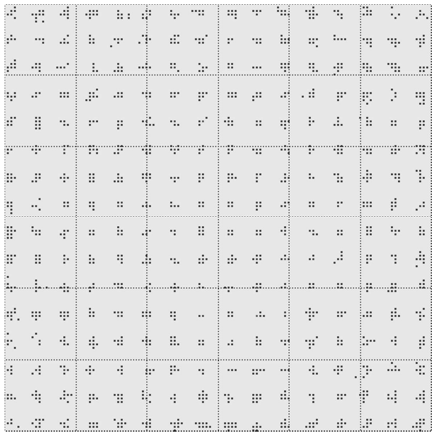


Рис. 4 Констеляційна діаграма сигналу з несною 850 МГц на виході макету при модуляції QAM-256.

Проведене дослідження вказує на високу якість передачі сигналу цифрового телебачення стандарту DVB-C макетом РРЛ терагерцового діапазону. Сигнали DVB-C з найменшою завадостійкістю (при модуляції QAM-256), проходячи через даний макет РРЛ терагерцового діапазону, демодулювалися за допомогою ресиверу HomeCast з якістю до 53%.

Література

1. Ільченко М.Ю. Передавальний та приймальний радіотракти радіорелейних систем терагерцового діапазону / Ільченко М.Е., Наритник Т. М., Радзіховскій В.М., Кузьмін С.Е., Лутчак А.В. // Цифрові технології № 17. – 2015. – с. 17-29. – Режим доступу: http://www.mitris.com/files/16-29.pdf.

УДК 621.396.946

ХАРАКТЕРИСТИКА БЕЗСПРОВОДНОЇ СИСТЕМИ ДЛЯ ДІАПАЗОНУ 240 ГГц

Приступчук Ю.А., Половий О.М., Шелковников Б.М.
Інститут телекомуникаційних систем НТУУ «КПИ»
E-mail: kyzon2008@gmail.com

Description of wireless system at a frequency of 240 Ghz

This paper presents the results of the wireless system at a frequency of 240 GHz with 128QAM modulation use, using a packet of AWR, and results of researches are provided.

Зростання пропускної здатності безпровідного зв'язку потребує нових способів зв'язку, які будуть в змозі передавати великі об’єми даних і не будуть впливати на існуючі системи. Системи, які задовольняють цим вимогам – це системи на основі транзисторів великої електронної рухомості (HEMT). Ця технологія отримала значний інтерес з боку як промисловості, так і наукових кіл, за рахунок можливості отримання високої концентрації електронів в дуже тонкому шарі, а також можливості керування концентрацією в каналі [1-4].

У даній статті наведені результати моделювання бездротової системи, що працює на частоті 240 ГГц із застосуванням HEMT технології в програмному пакеті AWR. Також проаналізовано вплив параметрів системи на якісні показники системи.

Схема системи зображена на рис. 1. На схемі передавач складається з наступних функціональних вузлів:

128QAM Digital Source - генератор випадкових даних на швидкості 28 Мб/с (хоч система здатна досягати швидкостей Гб/с, дана швидкість була вибрана для нагляднішого демонстрування результатів моделювання); Up Convert – вузько смуговий змішувач; QAM Transmitter - мікросхема модулятора QAM; AWGN – канал передачі сигналу. На виході модулятора виходить маніпулюваний сигнал з несучою частотою 240 ГГц (синтезатори та змішувачі входять до складу мікросхеми). Вид отриманого сигналу зображений на рис. 2. Для згладжування вихідного сигналу в модуляторі використовувався фільтр з «піднятою» косінусоідой з r = 0,35 [5].

В якості нелінійної моделі використовується модель підсилювача (GaAs HEMT) та змішувача. Показник підсилювача P1db прийнятий рівним 20 дБм. Коефіцієнт посилення був обраний рівним 10 дБ (з параметрів підсилювача фірми HITTITE HMC-AUH320). Розрахований вид амплітудної характеристики підсилювача та системи передачі зображений на рис . 3. Для змішувача була встановлена нижня межа пропускання 239,5 ГГц, а верхня – 240,5 ГГц відповідно. Максимальна пульсація в смузі пропускання становила 0,1 Дб, а кількість фільтрів реактивності рівна 9. При передачі сигналу для

каналу не було встановлено додаткових втрат (параметр Loss = 0).

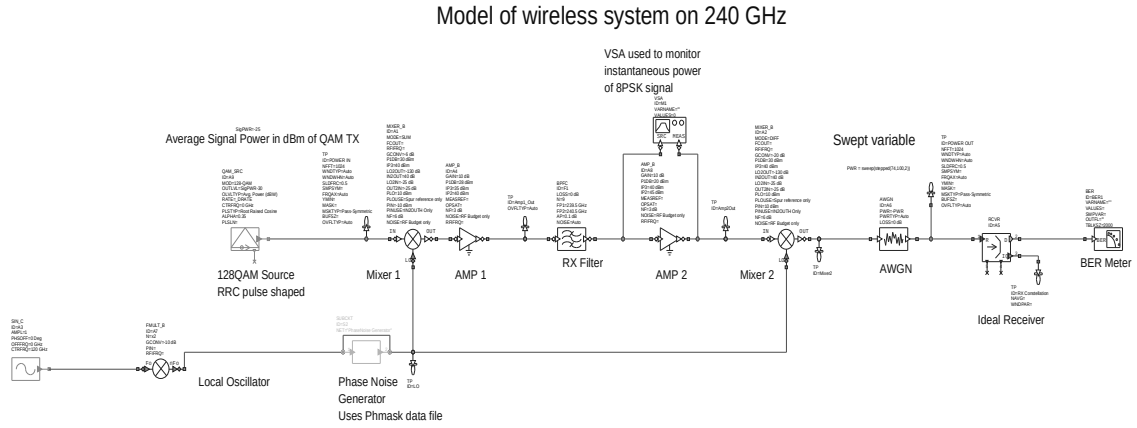


Рис. 1 Схема радіосистеми на частоті 240 ГГц із застосуванням 128QAM модуляції.

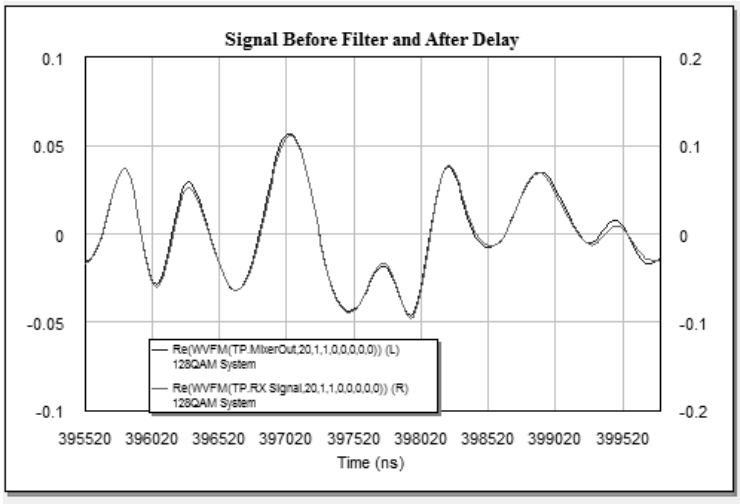


Рис. 2 QAM сигнал на виході модулятора.

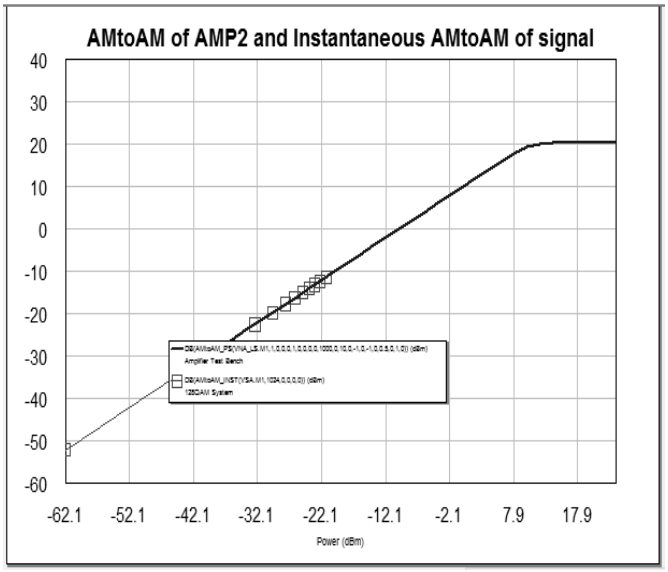


Рис. 3 Амплітудна характеристика системи.

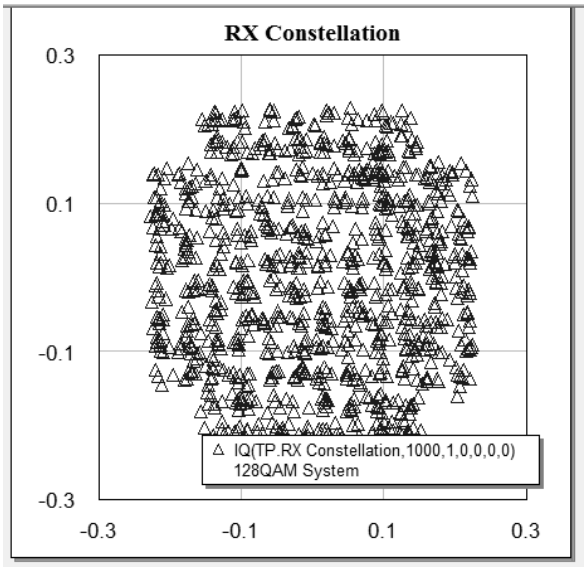


Рис. 4 Фазовий простір 128QAM.

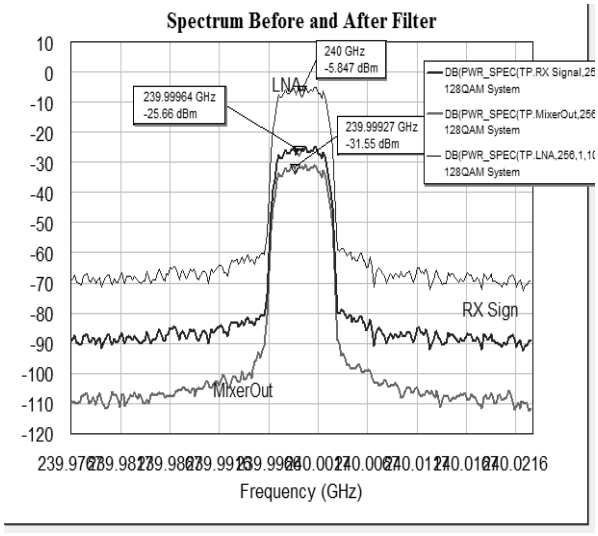


Рис. 5 Спектри сигналу до і після фільтрів.

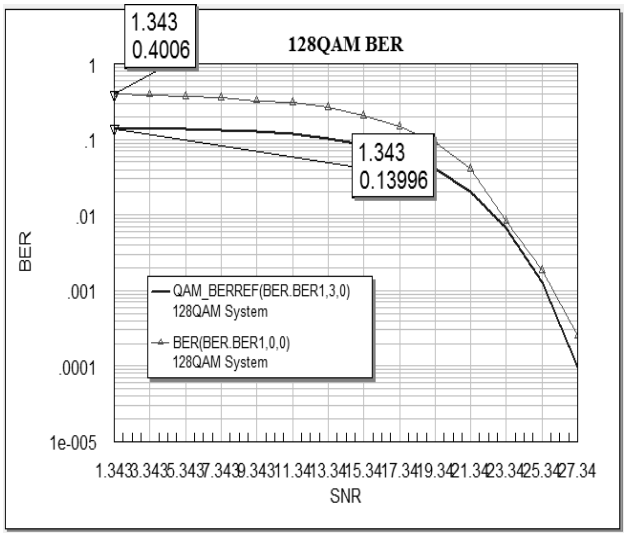


Рис. 6 Результати розрахунку BER.

Також тут можна варіювати загасання, що вноситься середовищем, впливаючи на якісні показники приймача. Так при значенні загасання рівному 50 дБ сузір'я даних зображені на рис. 4. Характеристика фільтра передавача і відповідні рівні сигналу до і після нього при великому вхідному сигналі на підсилювач зображені на рис.5. Результати розрахунку BER зображені на рис. 6.

У роботі була побудована схема радіосистеми на частоті 240 ГГц, з використанням 128QAM модуляції та із застосуванням технології HEMT. Проаналізовано вплив параметрів системи і видів модуляцій на якісні показники системи. На основі отриманих результатів можна пред'являти вимоги до окремих функціональних вузлів і подальшого їх проектування.

Література

1. IEEE P802.3ae 10Gb/s Ethernet Task Force (http://grouper.ieee.org/groups/802/3/ae/index.html)
2. Maas Stephen A. Nonlinear Microwave and RF Circuits. Boston: Artech House, 2003. 604 p.
3. Hirata Akihiko, Kosugi Toshihiko, Takahashi Hiroyuki 120-GHz-Band Millimeter-Wave Photoni Wireless Link for 10Gb/s Data Transmission // IEEE Transactions on micro-mave theory and techniquos. May 2006. Vol. 54. No. 5.
4. C. Jastrow, S. Priebe, B. Spitschan, J. Hartmann, M. Jacob, T. Kurner, T. Schrader, and T. Kleine-Ostmann, “Wireless digital data transmission at 300 ghz,”Electronics Letters, vol. 46, no. 9, pp. 661 –663, 29 2010.
5. H.-J. Song, K. Ajito, A. Hirata, A. Wakatsuki, T. Furuta, N. Kukutsu, and T. Nagatsuma, “Multi-gigabit wireless data transmission at over 200-ghz,” inInfrared, Millimeter, and Terahertz Waves, 2009. IRMMW-THz 2009. 34th International Conference on, sept. 2009, pp. 1 –2.

УДК 621.396.946

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ПЕРЕДАЧІ СИГНАЛУ ЦИФРОВОГО ТЕЛЕБАЧЕННЯ СТАНДАРТУ DVB-T2 ПО РАДІОРЕЛЕЙНІЙ ЛІНІЇ МЕТОДОМ КОМБІНОВАНОЇ МОДУЛЯЦІЇ

Авдєєнко Г.Л, Адамович О.М.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: oleg_adamovych@ukr.net

The research of digital television signal of the DVB-T2 standard transmission possibility via the radio relay line with combined modulation method usage

Practical substantiation of development of a new approach with the key feature of the analog radio relay lines with frequency modulation modem equipment adaptation to transmit TV signal of DVB-T2 standard on basis of the principle of double modulation COFDM/ FM is presented.

Швидкий розвиток електронних засобів масової інформації призводить до неухильного зростання передаваної інформації: цифрові телевізійні програми, Інтернет і.т.д. В Україні одним з найбільш поширених способів доставки телевізійних (ТВ) програм від столиці до обласних телевізійних центрів, в основному, залишаються лінії аналогового та цифрового радіорелейного зв'язку [1]. Також відомо, що відповідно до плану переходу на цифрове телевізійне мовлення (ЦТМ) – «Женева-2006», Україна взяла на себе зобов'язання до 17 липня 2015 року повністю перейти на цифрове телебачення (ЦТБ), остаточний перехід України на ЦТБ згідно розпорядження Національної Ради України з питань телебачення і радіомовлення відкладається орієнтовно на 2017 рік [2]. Тому виходячи із сказаного вище, постає питання пошуку рішень щодо модернізації та адаптації існуючої діючої мережі аналогових радіорелейних ліній зв'язку (РРЛЗ) для передачі по них цифрових потоків даних, зокрема сигналів цифрового телебачення стандарту DVB-T2. Вказане питання є актуальним, оскільки після відключення аналогового телебачення дані РРЛЗ залишаться розвантаженими і, відповідно, постане питання щодо їх демонтажу, або подальшого пристосування для передачі сигналів цифрового телевізійного мовлення (ЦТМ). Тому в цій статті запропоновано варіант практичної реалізації ідеї використання РРЛЗ, на базі радіорелейних станцій (РРС) «Комплекс МГ», з частотною модуляцією (ЧМ) для передачі радіосигналів ЦТМ стандарту DVB-T2.

Запропонований варіант практичного дослідження можливості застосування РРС з ЧМ для передачі радіосигналів ЦТМ стандарту DVB-T2 розглянемо на прикладі макета, спеціально створеного для цієї мети. Макет складається з 4-х основних частин (підсистем): перша частина – підсистема формування радіосигналу ЦТМ стандарту DVB-T2; друга частина – підсистема сполучення з модулятором модему Ц-2/8, третя частина – це типове обладнання РРЛЗ, тобто модеми Ц-2/8 і приймально-передавальні

блоки РРС «Комплекс МГ», з'єднані між собою поляризаційним хвилевідним атенюатором з можливою глибиною регулювання загасання від 0 до 50 дБ, який виконує роль еквівалента реальної лінії зв'язку, четверта частина – підсистема сполучення з демодулятором модему Ц-2/8 і високочастотним інтерфейсом ресивера кабельного ЦТМ стандарту DVB-T2.

Структурна схема макету для дослідження передачі радіосигналу ЦТМ стандарту DVB-T2 через РРЛЗ з ЧМ зображена на рис. 1.

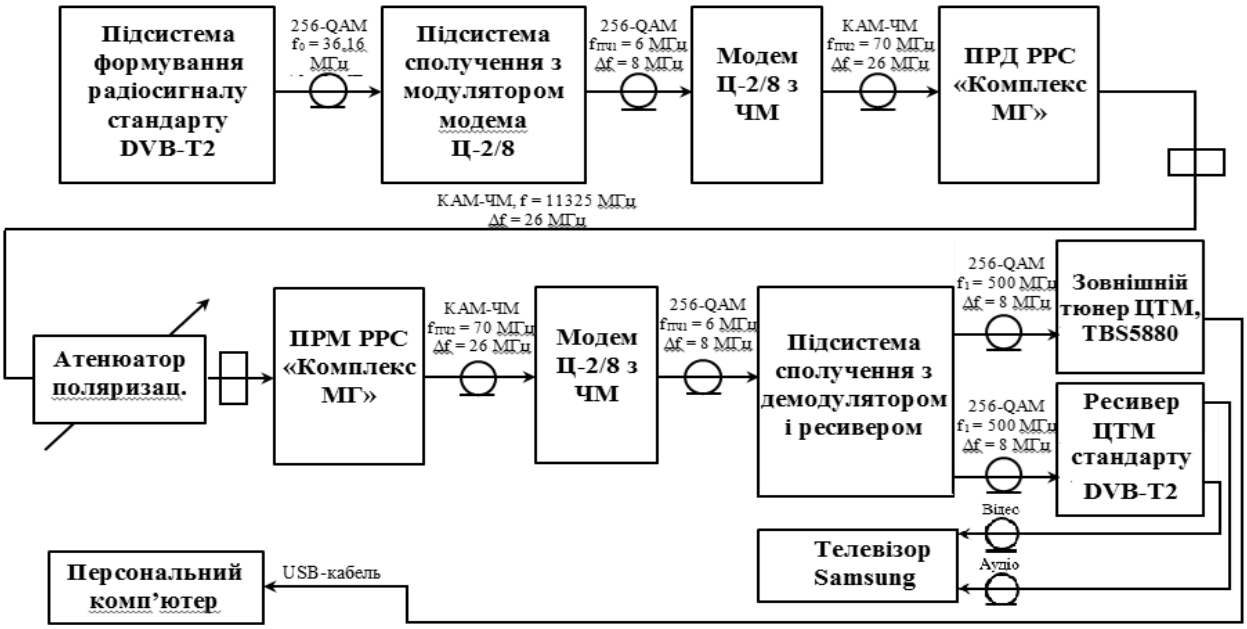
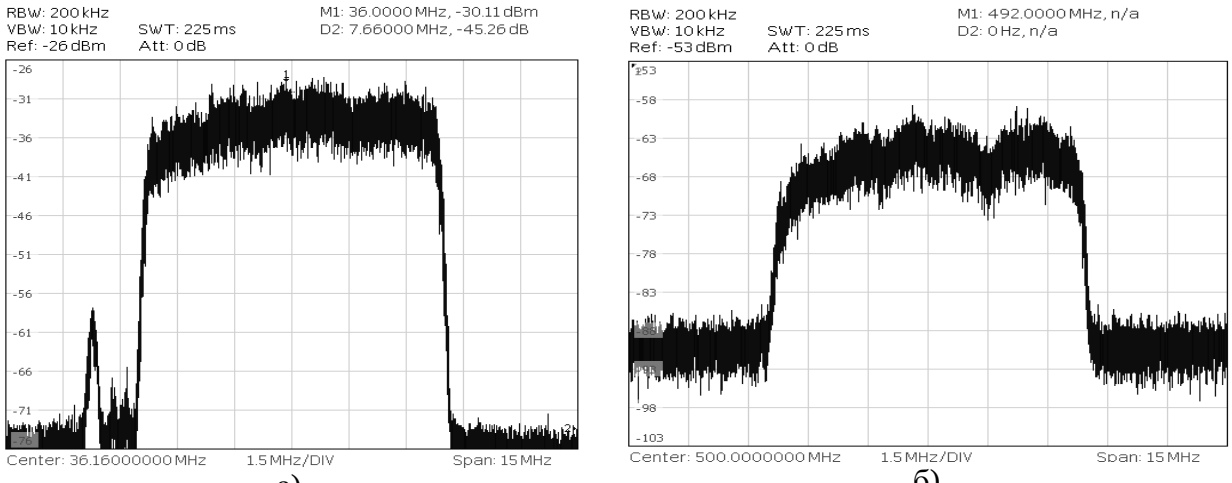


Рис. 1. Структурна схема макету для дослідження передачі радіосигналу ЦТМ стандарту DVB-T2 через РРЛЗ з ЧМ.



а) б)

Рис. 2. Спектрограми радіосигналу стандарту DVB-T2 після підсистеми формування сигналу стандарту DVB-T2 (а), на виході підсистеми сполучення з демодулятором і ресивером (б) та його сигнальне сузір'я на приймальному кінці (в).

В результаті дослідів, отримана якість сигналу, після проходження через макет становила 25 %, хоча на вході підсистеми формування сигналу стандарту DVB-T2 вона складала 100%. Такий показник зумовлений недосконалістю макета на якому проводилися досліди: малим динамічним

діапазоном підсилювачів, неідеальностями амплітудно-частотної характеристики фільтра низьких частот (ФНЧ), тощо. В подальшому відбуватиметься робота по вдосконаленню дослідного макета шляхом відповідного налаштування ФНЧ, підсилювачів ТВ сигналів, підбору необхідних провідників для більш якіснішого та надійнішого з'єднання елементів макету.

Незважаючи на відносно низьку якість отриманого сигналу на екрані монітора ПК та телевізора було отримано чітке зображення та звук, і відповідне сигнальне сузір'я ТВ сигналу стандарту DVB-T2 на приймальному кінці (див. рис. 3).

а) б)

Рис. 3. Зображення ТВ сигналу стандарту DVB-T2 на екрані ПК (а), та сигнальне сузір'я на приймальному кінці (б).

Результати отримані по закінченню виконання дослідження мають важливе і перспективне значення з точки зору подальшого вдосконалення та доповнення технічних знань в галузі телекомунікацій. Передбачається, що вказане технічне рішення скоротить кількість модуляторного обладнання стандарту DVB-T2, що дозволить заощадити кошти на побудову мережі ЦТМ. Практичні результати отримані під час проведення дослідження можуть бути використані:

1. Концерном «РРТ» та ТОВ «Зеонбуд» для забезпечення надійності трансляції ТВ програм стандарту DVB-T/T2 на проблемних частинах території України .

2. В навчальному процесі ІТС НТУУ КПІ при проведенні лабораторних робіт з кредитних модулів "Технології радіо- і телевізійного мовлення", "Передавльні та приймальні пристрої" та "Безпроводові телекомунікаційні системи-1".

Література

1. Проблемы и перспективы построения наземных эфирных сетей цифрового телевидения в Украине [Електронний ресурс]. - Режим доступу: http://www.mitris.com/files/pr.pdf.
2. Цифра відкладається. Телекритика [Електронний ресурс]. - Режим доступу: http://www.telekritika.ua/rinok/2015-06-10/108047.

УДК 621.3

РАЗВЕРТЫВАНИЕ МАЛЫХ СОТ ДЛЯ ЭНЕРГОЭФФЕКТИВНОЙ ГЕТЕРОГЕННОЙ СОТОВОЙ СЕТИ

Гордеева Д.С., Курдеча В.В.
Институт телекоммуникационных систем НТУУ «КПИ», Украина
E-mail: dariagordeeva1@gmail.com

Small cell deployment for energy-efficient heterogeneous cellular network

This article deals with the heterogeneous cellular network with small cells. There is hexagonal grid model for the deterministic deployment and Poisson process model is for the random deployment of small cells, which allow us to compare them. The result of this article is the analysis of energy efficiency of heterogeneous network.

В статье рассмотрена сотовая гетерогенная сеть с применением, малых сот. Использована модель гексагональной сетки для детерминированного развертывания и модель пуассоновского процесса для случайного развертывания малых сот, что дает возможность их сравнения. Результатом работы есть анализ энергоэфективности гетерогенной сети.

Взрывной рост спроса данных, обусловленный мобильными устройствами, представляет собой серьезную проблему для беспроводных сетей сотовой связи. Для увеличения емкости сети могут быть добавлены базовые станции (БС) малых сот к существующим сотовым сетям [1]. Они характеризуются малой мощностью, низкой стоимостью и размещены в общем канале в макросотах. Эти малые соты могут быть детерминировано развернуты оператором сети, например, микросоты, пикосоты или могут быть размещены случайным образом пользователями, т.е. фемтосоты.

В этой статье мы рассмотрим модель детерминированного развертывания и развертывание случайным образом малых сот в гетерогенных сетях. Мы будем ориентироваться на их развертывании в ограниченном пространстве в пределах одной макросоты. Детерминированное развертывание будет смоделировано в качестве гексагональной сетки, а случайное как пуассоновский процесс. После этого можно будет сравнить их энергоэффективность. Также рассмотрим модель объединения детерминированного и случайного развертывания и проанализируем ее энергоэффективность. Это поможет решить, какая из схем развертывания превосходит в плане повышения энергоэффективности, а также даст ли применение большего количества малых сот большую энергоэффективность.

Рассмотрим объединенный сценарий развертывания (рис. 1). На рисунке темный треугольник представляет собой БС макросоты, а маленькие полые треугольники - БС малых сот. БС макросоты расположена в центре ее зоны покрытия. Как видно, штрих-пунктиром наведены шестиугольники, это и

есть представление детерминированного развертывания, а все остальные БС, которые не находятся на шестиугольниках, расположены в произвольном порядке.

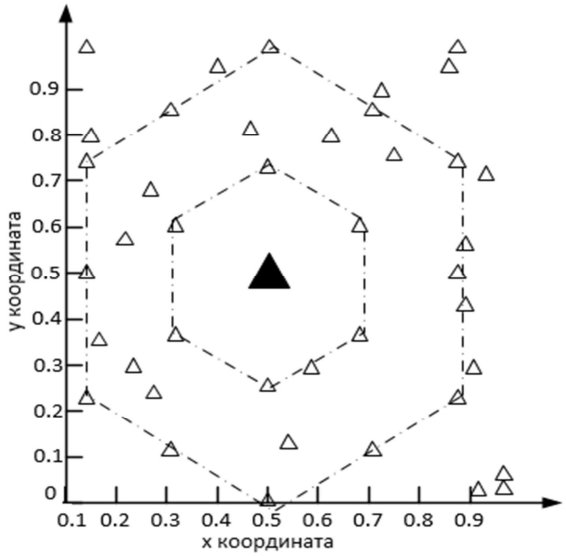


Рис. 1 Объединение двух моделей развертывания:
детерминированной и случайной.

В установке моделирования методом Монте-Карло возьмем следующее допущения: (I) зона покрытия макросоты нормирована на единицу площади; (II) местоположения АО генерируются в соответствии с пуассоновским процессом с интенсивностью 100; (III) так как переменная Пуассона может быть бесконечной, мы ограничиваем оба числа малых сот и АО до некоторых фиксированных значений, так что пуассоновский процесс сводится к биноминальному точечному процессу; (IV) мощность передачи малых сот равняется 1 и мощность передачи макросот - 100; (V) коэффициент потерь в пути $\alpha = 4$ и коэффициенты затухания $\beta = 1$.

Формула для энергоэффективости представлена следующим образом [2]:

$$\mathrm{EE} = \frac{\sum_{i=1}^{N_u}\sum_{j=1}^{N_s}\frac{B}{N_{y_j}}log_2\left(1+SIR_{x_i}\right)+\sum_{i=1}^{N_u}\frac{B}{N_{y'}}log_2\left(1+SIR_{x_iy'}\right)}{N_sP_s}$$

На рис. 2 представлен график зависимости энергоэффективности от количества АО и способа размещения БС малых сот.

Эффективность использования энергии, в сравнении различного количества БС малых сот для случайного, детерминированного и объединенного развертываний, повышает эффективность использования энергии для сотовой сети в детерминированном развертывании, в то время как при случайном развертывании, энергоэффективность, на самом деле, снижается после того, как плотность БС малых сот достигнет порогового значения. Это означает, что с увеличением числа БС малых сот, увеличение

скорости АО не может опережать линейное увеличение потребляемой мощности в БС. То есть, в случайном развертывании размещение БС малых сот не может быть оптимальным выбором для достижения более высокой энергоэффективности. В объединенной модели энергоэффективность является усредненной. В такой модели необходимо точно рассчитывать количество БС, так как это влияет на пороговое значение энергоэффективности.

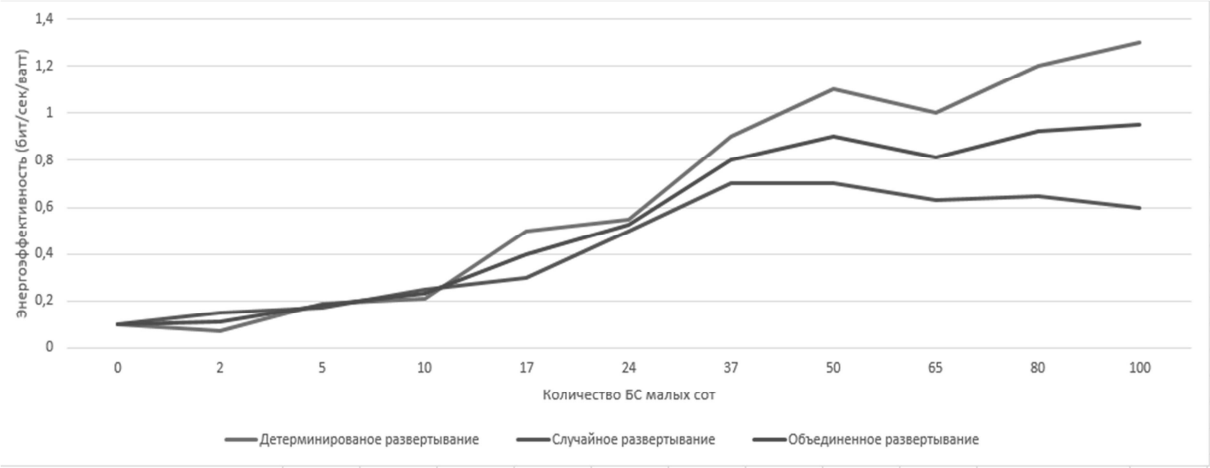


Рис. 2 Энергоэффективность сети в зависимости от количества мелких клеток с 100 АО

Проанализировавши энергоэффективность сети, можно сделать выводы, что детерминированная стратегия развертывания, как правило, лучше случайного развертывания и объединенного, так как в ней не возникают межсотовые помехи, в отличии от тех двух, где БС малых сот располагаются произвольно близко друг к другу и вызывают межсотовую интерференцию. Также, энергоэффективность при случайном и объединенном развертывании снижается, после того, как плотность БС малых сот достигнет порогового значения.

Литература

1. A. Ghosh, J. G. Andrews (2012). Heterogeneous cellular networks: From theory to practice. IEEE Communications Magazine, P. 54-64.
2. Gongchao Su, Lemin Li (2014). On the optimal small cell deployment for energy-efficient heterogeneous cellular networks. IEEE: Ubiquitous and Future Networks (ICUFN). P.172 - 175.
3. Kurdecha V.V., Zingaieva N.A. (2010). Aspects of basic network modernization for internetworking with devices based on SDR. International Crimean Conference - CriMiCo: Microwave & Telecommunication Technology. P. 518-519.

УДК 621.391

ОЦЕНКА ДИСПЕРСИИ ДАЛЬНОСТИ ДО ИСТОЧНИКА РАДИОИЗЛУЧЕНИЯ ПО РЕЗУЛЬТАТАМ ИЗМЕРЕНИЯ ФАЗОВЫХ СДВИГОВ ДЛЯ ВЫБОРА МАКСИМАЛЬНОГО КОЛИЧЕСТВА ЭЛЕМЕНТОВ АНТЕННОЙ РЕШЕТКИ

Цуканов О.Ф., Якорнов Е.А.
Институт телекоммуникационных систем НТУУ «КПИ»
E-mail:yakornov@its.kpi.ua

Dispersion range evaluation towards the radio source based on the results of phase shifts' measurements for selecting the maximum number of elements in antenna lattice

The maximum possible number of elements in the linear array antenna has been determined based on error dispersion estimation in determining the distance to the radio source, located in the Fresnel zone. At the same time the disambiguation problem of phase shifts measuring on the curvature of electromagnetic wave front has been solved in order to define the Fresnel contours.

В работе [1] рассматривается решение задачи определения местоположения источника радиоизлучения (ИРИ) при его нахождении в зоне Френеля по кривизне фронта электромагнитной волны (ЭМВ), принимаемой разреженной линейной антенной решеткой (АР), с помощью еще не нашедшего должного применения нового информационного параметра разности разностей фаз ($\Delta\Delta\psi$) между тремя разнесенными приемными антеннами решетки в предположении того, что фронт принимаемой ЭМВ является сферическим. В частности, показано, что этот параметр связан с дальностью до ИРИ. Однако применение систем на основе $\Delta\Delta\psi$ ограничено имеющейся неоднозначностью фазовых отчетов (когда $\Delta\Delta\psi$ становится больше 720^0).

Основываясь на подходе к устранению неоднозначности при оценке углового направления θ ИРИ по плоскому фронту ЭМВ, изложенному в [2], проанализируем возможности устранения неоднозначности для эквидистантой линейной АР, состоящей из $M+1$ приемных элементов (рис.1), которые находятся друг от друга на расстоянии половины средней длины волны $\lambda/2$ рабочего диапазона системы с АР в случае определения дальности R до ИРИ по кривизне фронта ЭМВ.

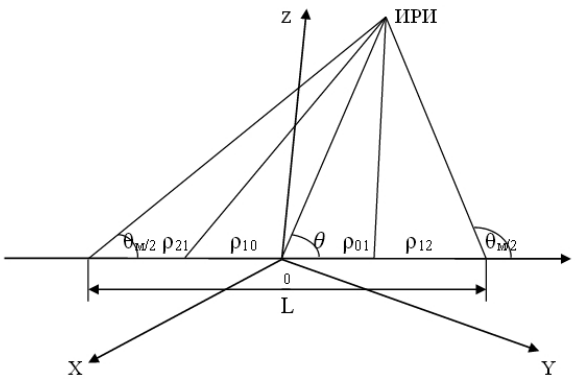


Рис.1

Однозначное измерение фазы сигнала ИРИ возможно когда

минимальная длина АР $L=\lambda$. Если $L>>\lambda$, то однозначное измерения возможно, если расстояние между элементами разреженной АР $\rho_{M0..}$, ρ_{10}, ρ_{01}, ρ_{02},...ρ_{0M} равно $\lambda/2$, при общем количестве антенн М+1. Нумерация элементов АР начинается с антенны расположенной точке 0 рис.1, а измерения углового направления θ и R производятся относительно центрального элемента решетки.

Чтобы при нумерации антенн избежать отрицательного номера, введем квадратичную нумерацию i^2 =1,4..(M/2-1)^2,(M/2)^2. Таким образом, сигнал принятый каждым элементом АР будет усиливаться в i^2 раз, усиление будет максимальным в крайних элементах и квадратично уменьшаться до единицы в центральном элементе, то есть получаем некую АР со "сферической апертурой" для определения R по результатам измерениям фазовых сдвигов ($\Delta\psi$) ЭМВ со сферическим фронтом. Одновременно полагаем, что АР имеет "линейную" апертуру, а фронт ЭМВ плоским, тогда задача определения $\Delta\psi$ по сферическому фронту волны приводится к известной задаче однозначного определения $\Delta\psi$ между элементами АР, только для измерения дальности до ИРИ.

Сигналом ИРИ $Y(R)$ являются значения набегов фаз ψ_i, i - ых элементов разреженной АР при известной, предварительно измеренной угловой координате θ.

$$Y(R)= \frac{2\pi}{\lambda}\frac{L^2 \sin^2\theta}{2R} + n(R), \quad (1)$$

где $n(R)$ - случайные флюктуации фазы.

В качестве оцениваемой величины берем параметр $\alpha=1/R$, называемый кривизной фазового фронта [2], тогда

$$Y(L, \alpha) = G\cdot\alpha\cdot L^2 + n(\alpha), \quad (2)$$

где $k = \frac{2\cdot\pi}{\lambda}$, $G = k\cdot\sin^2\theta/2$;

После дискретизации, запишем (2) в виде

$$\bar{Y}(L, \alpha)= \bar{X}(L, \alpha)+ \bar{n}(\alpha),$$

где $\bar{X}(L,\alpha)$- вектор ожидаемой реализации фазы в раскрыве АР.

Используя методику нахождения оценок по методу максимума правдоподобия для сигнала с полностью известными, кроме измеряемого параметра получаем:

$$ln[\bar{Y}(L, \alpha)] = \bar{Y}(L,\alpha)^T \Phi^{-1} \bar{X}(L, \alpha) - 0.5\bar{X}(L, \alpha)^T \Phi^{-1}\bar{X}(L,\alpha), \quad (3)$$

где Φ^{-1}- обратная корреляционная матрица фазовых флюктуаций сигнала.

Максимально правдоподобная оценка $\hat{\alpha}$ соответствует выражению

$$\hat{\alpha} = \bar{X}(L,\alpha)^T \Phi^{-1} X(L,\alpha)))^{-1} Y(L,\alpha)^T \Phi^{-1} X(L,\alpha) \quad (4)$$

где $X(L,\alpha)^T = G\cdot\cdot L^2/\,\mathrm{M}^2||(\mathrm{M}/2)^2\ (\mathrm{M}/2\text{-}1)^2$ .....2 1 0 1 2 .....$(\mathrm{M}/2\text{-}1)^2\ (\mathrm{M}/2)^2||$.

Полагая, что $\bar{X}(L,\alpha)^T \bar{X}(L,\alpha) = \frac{2\mathrm{G}^2\mathrm{L}^4}{M^4}\sum_{i=1}^{\frac{M}{2}} i^4$, а

$$\bar{Y}(L,\alpha)^T \bar{X}(L,\alpha) = 2\,\mathrm{G}^2\,\mathrm{L}\sum_{i=1}^{\frac{M}{2}} i^2(\psi_i - \psi_{i-1})/\mathrm{M}^2,$$

и с учетом [3] получим

$$\bar{X}(L,\alpha) = 4\,G^2L^4[\,(1/30)[\,(M/2)(M/2+1)(M+1)(3(M/2)^2+3(M/2)-1)]/M^4.$$

$$Y\,(L,\alpha)^T X(L,\alpha) = 2G^2\,L\sum_{i=1}^{M/2} i^2(\psi_i - \psi_{i-1})/M^2.$$

Обозначим, $\Delta\psi_i = \psi_i - \psi_{i-1}$ тогда

$$\hat{\alpha} = \frac{15M^2\sum_{i=1}^{M/2} i^2\Delta\psi_i}{G^2L\,(M/2)(M/2+1)(M+1)\left(\left(\frac{M}{2}\right)^2+3(M/2)-1\right)} \qquad (5)$$

Оценим значение σR^2 – дисперсию ошибки оценки дальности $\hat{R} = 1/\hat{\alpha}$.

$$\sigma R^2 = \pi L^2\left[\left(\frac{2\lambda\sin 2\theta}{\Delta\psi}\right)^2\sigma\theta^2 + \left(\frac{\sin^2\theta}{\Delta\psi}\right)^2\sigma\lambda^2 + \left(\frac{\lambda\sin^2\theta}{\Delta\psi^2}\right)^2\sigma\Delta\psi^2\right], \qquad (6)$$

где: $L = (M+1)\,\lambda/2$, σR^2 - дисперсия ошибки измерения дальности, $\sigma\theta^2$, $\sigma\lambda^2$, $\sigma\Delta\psi^2$ - дисперсия ошибки измерения θ, λ, $\Delta\psi$ - соответственно.

Величины $\sigma\theta^2$, σf^2, $\sigma\Delta\psi^2$ определяются техническими характеристиками устройств измерения параметров θ, λ, $\Delta\psi$. Значение $\sigma\theta^2$ определяет квадрат ошибки измерения углового направления θ, $\sigma\lambda^2$ - квадрату ошибки измерения длины волны ИРИ, а $\sigma\Delta\psi^2$ определяется квадратом ошибки измерения фазового сдвига $\Delta\psi$.

Ввиду малого значения первого и второго слагаемого ими можно пренебречь. Значение σR^2 определяется длиной АР L и погрешностью измерения $\Delta\psi$. Итак чем больше L, тем больше дисперсия ошибки измерения дальности σR^2, причем эта зависимость квадратичная.

n	M+1	σR^2 [м^2]
1	5	0.36
2	6	0.49
3	9	1.2
4	12	1.7
5	15	2.6

Выражение (6) позволяет сделать вывод о конфигурации АР. Зависимость σR^2 от количества элементов АР M для λ=1м. приведены в таблице. Анализ таблицы показывает: чтобы значение дисперсии σR^2 не превышало 1м^2 максимальное число приемных элементов АР не должно превышать 9.

В этом случае можно также достичь максимальной дальности измерения (увеличения границы зоны Френеля) при минимальной дисперсии ошибки.

Литература

1. Авдеенко Г.Л., Федоров В.И., Якорнов Е.А. Определение местоположения источника радио излучения по кривизне фронта электромагнитной волны. Известия вузов. Радиоэлектроника. - 2008. № 3. – с. 3-11.
2. Патент № 2322681 (Россия) Способ определения дальности до забрасываемого передатчика помех и устройство для его реализации. М. кл. G01S 3/00 // Боровиков С.Г., Ястребов Ю.В.
3. Интегралы и ряды. Прудников А.П., Брычков Ю.А., Маричев О.И. - М.: Наука, 1981, с.597.

УДК 621.396.43

ДОСЛІДЖЕННЯ МЕРЕЖІ ШИРОКОСМУГОВОГО АБОНЕНТСЬКОГО ДОСТУПУ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ В ТЕРАГЕРЦОВОМУ ДІАПАЗОНІ

Наритник Т.Н., Єрмаков А.В.,
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: yermak_antonio@ukr.net
Казіміренко В.Я., Сайко В.Г.
Державний університет телекомунікацій, Україна
E-mail: vkazim2@gmail.com

Research broadband subscriber access to information resources in a range in the terahertz

Described technical solutions and presents the results of studies create a wireless network broadband terahertz range of technology-based Wi-Fi 802.11 n standard information services to cover areas with expanded service area. It is shown that sectoral solutions providing the necessary service area potentially allows more efficient use of resources provided by broadband and implemented in each sector to provide the best information resource subscribers.

Вичерпаність частотного ресурсу при необхідності підвищення щільності дислокації абонентів та розширення зони обслуговування робить актуальним дослідження використання неліцензійного частотного діапазону (НД) для надання широкосмугового безпроводового доступу до інформаційних ресурсів [1]. В зв'язку з цим проведення досліджень створення безпроводової мережі широкосмугового доступу із використанням міліметрового та терагерцового частотного діапазону для покриття інформаційними послугами території з розширеною зоною обслуговування є актуальною задачею. Тому нами досліджувалась широкосмугова мережа абонентського доступу до інформаційних ресурсів терагерцового діапазону , створена на базі центральної станції, яка надає послуги безпроводового широкосмугового доступу. Технічне рішення системи базується на технології МІТРІС[2], при цьому абонентська мережа реалізується на стандарті 802.11n. Складові частини такої абонентської мережі найбільш сприятливі на сьогодні з точки зору вартості та якості реалізації послуги. .

Канали мережі, якою підключаються вузли доступу до центральної станції (мережа bakhaul) функціонують в неліцензійному частотному діапазоні. Приймально-передавальні засоби центральної станції створені на базі технічного рішення [3]. На базі технічних рішень [4-6] розроблена система [7], в якій по каналах мережі bakhaul підключаються вузли доступу локальної безпроводової абонентської мережі до центральної станції, а приймально-передавальна апаратура підключається в форматі Ethernet до вузла магістральної інформаційної мережі. Для оптимізації розподілу наданого інформаційного ресурсу використовується технічне рішення [8]. Запропоноване технічне рішення дозволяє створити опорну мережу, яка

надає можливість реалізувати доступ абонентських комп'ютерів до зовнішніх інформаційних мереж. Мережа абонентських комп'ютерів підключається до безпроводової локальної мережі, яка створюється засобами точки доступу, дислокованої в абонентській станції мережі на базі запропонованої технічним рішенням системи UMDS-TH [8]. При цьому передбачається використання неліцензійного (безоплатного) частотного діапазону в каналах мережі bakhaul, що понижує вартість послуг, спрощує процедуру отримання дозволу та знімає дефіцит частотного ресурсу.

Рішення цієї проблеми особливо важливе в умовах слаборозвинутої комунікаційної інфраструктури (наприклад, підключення до Інтернету абонентів в сільських регіонах, де кількість телефонних каналів мала, а якість їх вкрай низька, крім того зв`язок з сервером провайдера доводиться підтримувати по каналам міжміського зв`язку).

В якості приймально-передавальної апаратури – засобів передавання інформації по запиту абонентської станції та приймання запиту створено формувач інформаційного потоку для каналу зв'язку із підвищеною спектральною ефективністю та пропускною здатністю [8]. В блоці такого формувача використовуються технічні рішення, що базуються на елементах в вигляді чіпу. Вхід передавальної та вихід приймальної схеми в складі даного чіпу – бітовий потік в форматі Ethernet, а вихід передавальної та вхід приймальної схеми в складі даного чіпу – символьний потік на частоті в діапазоні біля 2 або 5 ГГц. Модуляція та демодуляція може програмно перебудовуватися від BPSK до QAM-64. Смуга отриманого сигналу складає 40 МГц. При цьому швидкість в каналі зв'язку складає 150Мбіт/с.

Підвищення спектральної ефективності досягається використанням багатопозиційної модуляції (QAM-64). Подальше підвищення швидкості в каналі зв'язку досягається створенням блоку, що виконує кодування та модуляцію потоку в форматі Ethernet із розподілом по суміжних частотних смугах та об'єднанні їх в загальний багаточастотний потік в передавальній частині та розподілу по вихідних частотних смугах із подальшою їх демодуляцією, маршрутизацією та формуванням Ethernet інтерфейсу в приймальній частині.

До складу приймально-передавального формувача, що складається із приймального та передавального трактів, введено n приймально-передавальних блоків в форматі чіпа, в передавальній частині якого є кодер, модулятор, підвищуючий частотний конвертор, за допомогою яких формується n окремих частотно рознесених потоків, які об'єднуються в загальний інформаційний потік, а приймальна частина включає декодер, демодулятор, понижуючий частотний конвертор, кожен із n приймальних блоків підключаються до частотного розгалужувача прийнятого загального інформаційного потоку. Таке технічне рішення дозволяє створення каналу зв'язку в необхідному терагерцовому частотному діапазоні, наприклад, методом гетеродинного перетворення до потрібного рівня. в Для збільшення розміру зони покриття використовуються приймальні та передавальні антени із коефіцієнтом підсилення до 50дБ. Кількість секторів зони обслуговування,

їх формування на оптимальне надання інформаційного ресурсу абонентам в кожному секторі визначається по результатам дослідження зони обслуговування.Створення мультиплексів меншого розміру ніж сумарний, що доводиться до абонента, дозволяє підвищити ефективність використання наданого інформаційного ресурсу.

Оскільки сигнал терагерцового діапазону при розповсюдженні в ефірі підлягає впливу значних втрат, то антени, що підключаються до лінійних трактів на стороні передачі і приймання мають значення направленості порядку 50дБ. Тобто кут розкриву діаграми спрямованості складе біля $1^0 \ldots 2^0$. При використанні окремих антен для кожного мультиплексу, і при співпаданні напрямку їх спрямованості сумарна територія покриття може бути збільшена на величину до двох раз. Тобто при використанні 8 окремих частотних потоків кут зони покриття може бути збільшений в порівнянні із випадком використання однієї антени в 16 раз і загальний кут покриття складе біля 24^0 при куті покриття однією антеною біля 1.5^0.

На основі запропонованих технічних рішень і отриманих результатів досліджень безпроводової мережі широкосмугового доступу до інформаційних ресурсів показано, що в терагерцовому діапазоні за рахунок спектрального забезпечення необхідної зони обслуговування можна потенційно підвищити ефективність використання наданого інформаційного ресурсу та реалізувати оптимальне надання в кожному секторі інформаційного ресурсу абонентам.

Література

1. Кравчук С.О. ,Наритник Т.Н., Телекомунікаційні системи и терагерцового діапазону Монографія.-Житомир.:- .:ФОП «Євенок О.О.».-2015.-394с.
2. Деклараційний патент України №51495А, дата публікації 15.11.02р. «Мікрохвильова інтегрована телерадіоінформаційна система МІТРІС-ІНТ» з пріоритетом від 12.04.2002р.
3. Патент України на корисну модель №84923, дата публікації 25.11.2013р., Бюл.№21 «Приймально-передавальний формувач інформаційного потоку для каналу зв'язку із підвищеною спектральною ефективністю та пропускною здатністю» з пріоритетом від 11.11.2013 р.
4. Патент України на корисну модель №97537, дата публікації 25.03.2015р., Бюл.№6 «Мікрохвильова інформаційна система надання послуг передачі даних із використанням терагерцового діапазону» з пріоритетом від 22.08.2014 р.
5. Патент України на корисну модель №93139, дата публікації 14.10.2014р., Бюл.№8 «Канал передачі даних в терагерцовому діапазоні з пропускною здатністю більше 1 Гбіт/с» з пріоритетом від 25.02.2014 р.
6. Патент України на корисну модель №104299, дата публікації 25.01.2016р., Бюл.№2 «Канал безпроводового широкосмугового абонентського доступу до інформаційних ресурсів із використанням каналу в терагерцовому діапазоні» з пріоритетом від 25.06.2015 р.
7. Заявка на корисну модель України U2015 12889 від 25.12.2015 р. «Телерадіоінформаційна система широкосмугового мультисервісного радіодоступу з підвищеною пропускною здатністю».
8. Заявка на корисну модель України U201600935 від 05.02.2016 «Мікрохвильова система широкосмугового безпроводового доступу з підвищеною щільністю покриття зони обслуговування UMDS-TH».

УДК 621.391

ПРОДУКТИВНІСТЬ СЕРВІСІВ, ЩО НАДАЮТЬСЯ МОБІЛЬНИМИ ОПЕРАТОРАМИ

Лазарєв К. Д., Лісковський І. О.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: exort@ukr.net

Performance of services, provided by mobile operators

This article shows a brief performance analysis of basic services that provide mobile communication. The rapid development of radio-access technology for mobile terminals provides operators a wide range of services. The aim of the research is to find the method of measuring influence on service quality, caused by raise of service traffic, generated by subscribers using those services.

Стрімкий розвиток мереж мобільного зв’язку, а особливо – мереж радіодоступу, дає змогу операторам більш широко використовувати можливості сучасний мобільних терміналів. Кількість сервісів в умовах жорсткої конкуренції зростає щодня, а з ними – трафік, що генерують мобільні термінали.

Для якісного аналізу продуктивності сервісів, іх класифікуюсть у наступні:

- Сервіси підмережі комутації каналів (CS);
- Сервіси підмережі комутації пакетів (PS).

До першої категорії відносять основну послугу мереж мобільного зв’язку – передачу голосу. Сучасні вимоги до якості передачі голосового трафіку набагато вищі від тих, що були заявлені у стандартах [1], що призводить до широкого зросту трафіку. Останні тенденції показують, що базові станції стандарту GSM, підключені до мережі за допомогою TDM-з’єднань не витримують навантажень та не задовольняють якісним параметрам. Тому поступово відбувається їх заміна на нове обладнання, що пітримує підключення до мережі через IP-з’єднання.[5]

До сервісів пакетної передачі даних відносять:

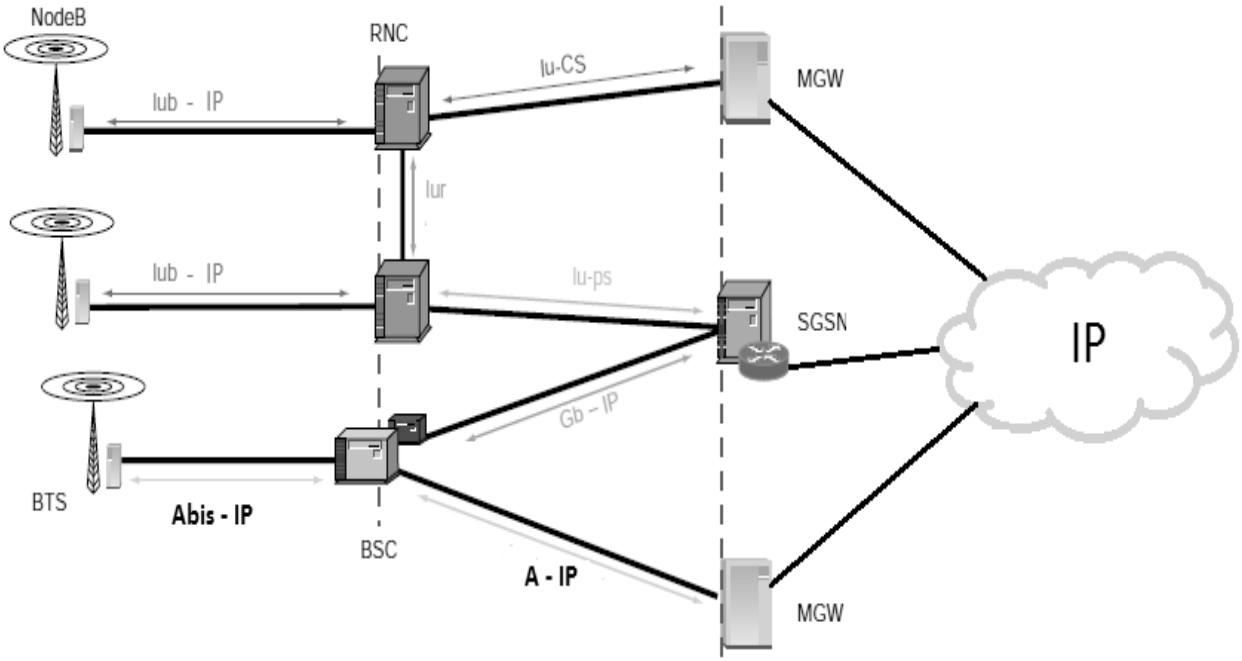
Передача голосових повідомлень - вимоги, що пред'являються до втрати інформації, по суті, такі ж як для передачі неперервного голосу, але ключова різниця – у низких вимогах до затримки, що викликане почерговою передачею повідомлень.

Дані – незважаючи на деякі виключення, з точки зору користувача основною вимогою для будь-якої програми передачі даних, є гарантована відсутність страти інформації. У той же час – відсутні чіткі стандарти для рівня затримки. Таким чином, кожен додаток самостійно визначає дозволений рівень затримки.[4]

Перегляд веб-сторінок - з точки зору користувача, основним фактором продуктивності є час завантаження сторінки. У сучасних мережах прийнятним є значенния 2-3 секунди, проте рекомендується його зменшення до 0.5 секунд.

Першочергові транзакційні послуги - основні вимоги продуктивності для даного сервісу – захищеність інформації, що передається та час проведення транзакції. Значення 2-4 секунди є прийнятним для більшості користувачів.[3]

Запровадження нового сервісу на мережі може призвести до перенавантаження каналів передачі трафіку і негативно вплине на якості надавання усіх інших сервісів.



Першим етапом запобігання данним ситуаціям є заміна обладнання із низьким рівнем пропускної здатності. Перехід до повної IP-інфраструктури дозволить зменшити ризик виникнення перенавантажень.[2]

Найбільш ефективним методом запобігання перенавантаженням є прогнозування трафіку на мережі. Детальний аналіз продуктивності сервісів дозволить операторам заздалегіть підготувати можливу

Література

1. Специфікація 3GPP TS 22.105 version 13.0.0 Release 13 “Services and service capabilities”.
2. *Vinod Joseph, Brett Chapman,* “Deploying QoS for Cisco IP and next generation networks : the definitive guide” – Elsavier , TK5105.5956.J67, 2009 – 99c.
3. *Kun I. Park* “QOS in packet networks” – Springer Science, 2010 – 119 c.
4. *Daniel A. Menasce , Virgilio A.F. Almeida,* “Capacity Planning for Web Services: Metrics, Models, and Methods”, – 2007 -299 c.
5. Mishra A. R. ,“Fundamentals of Cellular Network Planning and Optimization” – John Wiley & Sons – 2008, 322 c.

УДК 621.396

АНАЛІЗ ІСНУЮЧИХ ТЕХНІЧНИХ РІШЕНЬ ТА ОБҐРУНТУВАННЯ ВИБОРУ РАДІОМОДУЛЯ ДЛЯ ПОБУДОВИ ПРИЙМАЧА СИГНАЛІВ СИСТЕМ СУПУТНИКОВОЇ РАДІОНАВІГАЦІЇ GPS ТА ГЛОНАСС

Дудник А. В., Авдєєнко Г. Л.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: angie_dudnyk@ukr.net

The analysis of existing technological solutions and the reasoning of GPS/GLONASS radiomodules selection for satellite navigation receiver construction

In this article, producers of modern navigation modules are analyzed. The problem of selection radio modules GPS, GLONASS satellite navigation systems are described and solved.

Значимість розробки приймача супутникової радіонавігації систем GPS та GLONASS, полягає у підвищенні надійності визначення координат об’єкту (наприклад, транспортного засобу), особливо в умовах міської забудови та гірської місцевості, що досягається шляхом визначення місцеположення по радіосигналах не однієї, а двох систем супутникової навігації (GPS+GLONASS). Передбачається, що розроблений навігаційний приймач за своїми технічними характеристиками буде перевищувати навігаційні приймачі (в першу чергу по енергоспоживанню), що застосовуються в сучасних системах диспетчеризації транспортних засобів. Використання радіосигналів двох систем супутникової навігації в свою чергу дозволить з одного боку удосконалити навігаційний сегмент вказаних систем, а з другого боку – зменшити ймовірність відмови навігаційного обладнання, обумовленої неможливістю приймання сигналів від навігаційних супутників.

При конструюванні приймача супутникової системи радіонавігації GPS/ ГЛОНАСС важливим етапом є вибір радіомодулів.

В даній доповіді розглянуто основні задачі, що необхідно виконати при виборі радіомодулів для побудови приймача системи супутникової радіонавігації GPS/GLONASS, а саме:

1. *Пошук фірм-виробників* навігаційних (GNSS) радіомодулів для прийому сигналів GPS/GLONASS
2. *Формулювання критеріїв вибору* GNSS радіомодулів для розробки навігаційного приймача
3. *Вибір GNSS радіомодулю* відповідно до визначених критеріїв

Загальна кількість фірм-виробників приймальних модулів систем супутникової радіонавігації, серед яких здійснюється пошук за допомогою мережі інтернет, складав 30 шт., а саме (див. табл.1).

Відповідно до адрес сторінок фірм-виробників, що наведені в табл.1, необхідно проаналізувати технічну документацію приймальних модулів систем супутникової радіонавігації.

Табл.1 Перелік фірм-виробників навігаційних модулів.

№ п/п	*Назва фірми-виробника*	*Адреса в мережі Інтернет*
1	Trimble	www.trimble.com
2	Transystem inc.	www.transystem.com.tw
3	Locosys Technology	www.locosystech.com
4	GeoStar Navigation	www.geostar-navigation.com
5	U-blox	www.u-blox.com
6	4D systems	www.4dsystems.com.au
7	LeadTek	www.leadtek.com
8	Skylab	www.skylab.com.cn
9	SkyTraq	www.skytraq.com.tw
10	Navman wireless	www.navmanwireless.com
11	REYAX	www.reyax.com
12	GlobalSat	www.globalsat.com.tw
13	SIRF technology inc.	www.sirf.com
14	NovAtel inc.	www.novatel.com
15	Tyco Electronics	www.te.com
16	Sierra Wireless	www.sierrawireless.com
17	MicroStack	www.microstack.org.uk
18	GlobalTop	www.gtop-tech.com
19	Навиа	www.naviaglonass.ru
20	EverMore Technology	www.emt.com.tw
21	Quectel	www.quectel.com
22	ООО НВС «Навигационные технологии»	www.navitech.ru
23	Telit Wireless Communication	www.telit.com
24	NavSync	www.navsync.com
25	Orcam Systems	www.orcam.eu
26	Antaris	www.u-blox.com
27	Atheros Communications	www.qca.qualcomm.com
28	LinX Technologies	www.linxtechnologies.com
29	eRide	www.eride.com
30	SimCom	www.sim.com

Основними критеріями, відповідно до яких здійснений відбір навігаційних приймальних модулів були:

1. Струм споживання навігаційного модуля $I_{supply} \leq 40$ мА;
2. Час першого визначення місцеположення (TTFF, Time-to-first fix) $t \leq 32$ сек;
3. Висока точність визначення координат (CEP <2,5 м);
4. Підтримка супутникової системи диференціальної корекції EGNOS;
5. Підтримка обробки сигналів декількох систем супутникової навігації (GPS, ГЛОНАСС, Galileo).

Для закупівлі модулів навігаційних приймачів проведено аналіз наявності на ринку України електронних компонентів та аналіз ринку ближнього зарубіжжя фірм-постачальників, у яких є в наявності необхідний модулі. Крім того, здійснений аналіз та складання переліку додаткового устаткування, яке необхідно закупити для створення макетів навігаційних приймачів. В результаті проведеного аналізу технічних характеристик навігаційних модулів встановлено, що всім трьом критеріям відповідає модуль SIM68M фірми SIMCom.

Відповідно до документації навігаційного модулю SIM68M структурна схеми макетів з використанням пасивної GPS антени матиме вигляд (див. рис. 1).

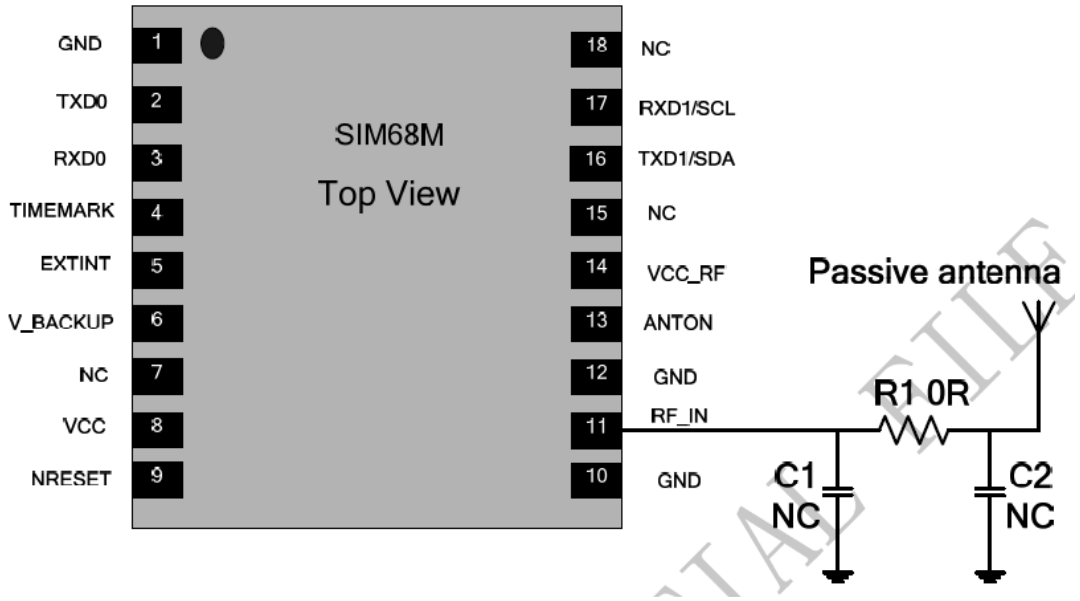


Рис. 1 Спрощена структурна схема навігаційного приймача на базі модуля SIM68M.

Задача вибору радіомодулю для побудови приймача сигналів систем супутникової радіонавігації GPS та ГЛОНАСС виконана. Навігаційний радіомодуль SIM68M задовольняє всім вимогам.

Література

1. Физические принципы работы GPS/ГЛОНАСС – Новосибирск: ГОУ ВПО "СГГА", 2009. – 87 с.
2. MT System Электронные компоненты [Електронний ресурс] – Режим доступу до ресурсу: http://www.mt-system.ru/store/13236/gps-priemniki-simcom.
3. SimCom [Електронний ресурс] – Режим доступу до ресурсу: www.sim.com.

УДК 612.396

ДОСЛІДЖЕННЯ ФУНКЦІОНАЛЬНИХ МОЖЛИВОСТЕЙ НАВІГАЦІЙНИХ ПРИЙМАЧІВ СИГНАЛІВ GPS/GLONASS

Солянікова В.Ю., Дудник А.В., Авдєєнко Г.Л.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: leka-br@mail.ru

The investigation of functional capabilities of navigational GPS/ GLONASS receivers

This paper analyzes which software are the most convenient to use in education process for learning the basic parameters and operating modes of navigation receivers of GPS / GLONASS signals.

Найбільш поширеними у світі є дві супутникові системи радіонавігації – це GPS (Global Positioning System) та ГЛОНАСС (Глобальна Навігаційна Супутникова Система). На сьогоднішній день ці системи дають можливість транспортного моніторингу автомобілів, потягів, літаків та інших рухомих об'єктів, які оснащені навігаторами. Тому це дозволяє відслідковувати і контролювати їх рух, спостерігати за маршрутом, швидкістю та іншими параметрами. Приймачі GPS/ГЛОНАСС використовуються також у міському та сільському господарстві. У міському господарстві це дає змогу легко і швидко знайти місце аварії в газових, водяних і каналізаційних трубопроводах, в сільському – координатне забезпечення полів. Також ці системи широко використовуються в картографії, археології, геодезії, стільниковому і волоконно-оптичному зв'язку та інших сферах людської діяльності[1].

Для підвищення рівня підготовки студентів в технічних ВУЗах телекомунікаційного профілю актуальною стає задача вивчення функціональних можливостей навігаційних приймачів, наприклад, за допомогою створеного макету навігаційного приймача, принцип дії та дослідження якого відображено в даній доповіді.

Для побудови даного макету було використано широко розповсюджений на ринку електронних компонентів України радіомодуль SIM68V компанії SIMCom [2]. Цей навігаційний приймальний модуль має наступні параметри:

- Робоча частота - 1575,42 МГц;
- Тип приймача: 99 каналів захоплення та 33 каналів слідкування;
- Чутливість в режимах: слідкування – 167 dBm, захоплення – 160 dBm, «холодного старту» – 148 dBm;
- Час першого запуску в режимах: «холодний старт» – 28 с, «теплий старт» – 26 с, «гарячий старт» < 1 с;
- Точність визначення координат – 2,5 м;
- Точність визначення швидкості – 0,1 м/с;
- Резервне джерело енергії: 2,3 – 4,6 В;
- Споживчий струм в режимах: захоплення – 34 мА, слідкування – 30 мА, адаптивний – 340 мкА, backup – 14 мкА;

- Підтримує: GPS, ГЛОНАСС, Galileo, QZSS;
- Підтримує супутникову корекцію: WAAS, EGNOS, GAGAN, MSAS;
- Автоматично придушує завади;
- Малошумлячий підсилювач інтегрований всередину приймача;
- Має асинхронний інтерфейс передачі даних;
- Працює по протоколу NMEA;
- Розмір: 16*12,2*2,4 мм.

У макеті приймача використовується дводіапазонна керамічна пасивна патч-антена фірми AMOTECH з розмірами 25*25*4 мм. Діапазон частот 1575-1608 МГц. Коефіцієнт підсилення – 3,5 дБ [3]. Схема макету навігаційного приймача, що досліджувався зображена на рис. 1.

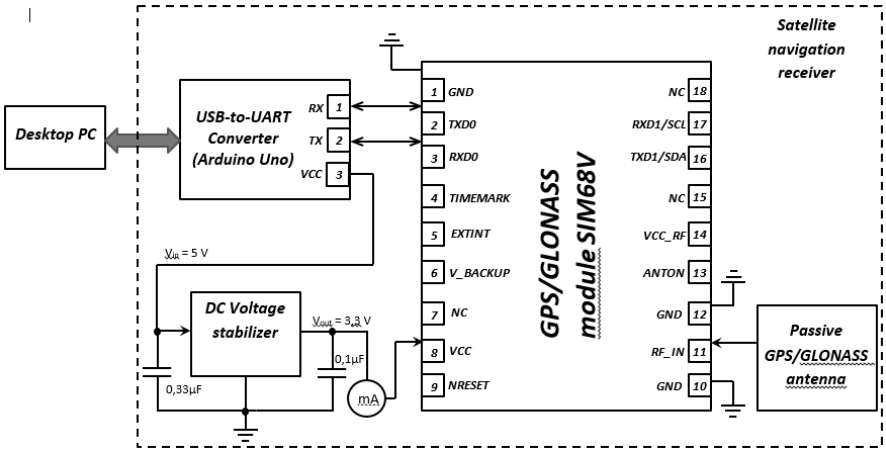


Рис.1 Схема макету навігаційного приймача

Більшість виробників модулів для навігаційних приймачів зазвичай розробляють відповідне програмне забезпечення, яке дає змогу протестувати основні параметри і режими модуля з використанням спеціальних налагоджувальних плат (Evaluation Kit або Evaluation Board). Оскільки усі навігаційні модулі видають інформацію в одному і тому ж протоколі NMEA, то програмне забезпечення одного виробника можна використовувати як для тестування модулів даного виробника, так і для модулів іншого виробника.

У результаті тестування навігаційного приймача виявлено, що найбільш повним функціоналом володіють наступні програмні засоби: U-center ver. 8.15 фірми U-blox; SIMCom GPS Demo ver. 3.0 фірми SIMCom; Fastrax Workbench ver. 5 фірми U-blox; GPSFox ver. 0.97 фірми Locosys; Trimble Studio ver. 1.33 фірми Trimble; GeoSDemo ver. 3.03 фірми GeoStar; Навиа ГЛОНАСС+GPS ver. 1.10.0.197 фірми «Навиа»; SkyTraq ver. 0.4.713 фірми SkyTraq; Linx Master Development System фірми Linx Technolodies.

У результаті дослідження було виявлено, що немає універсального програмного забезпечення, яке давало б змогу зробити усі необхідні виміри: в одних програмах є можливість вимірювати одні параметри, а в інших – інші. Кожний програмний продукт має як переваги перед іншими, так і недоліки.

Так як метою роботи є підвищення рівня обізнаності студентів у цій темі, то для роботи над даною доповіддю було обрано програмне забезпечення Fastrax Workbench ver. 5. Ця програма достатньо проста для

розуміння і зручна у використанні. На думку авторів, вона дає достатню кількість інформації для дослідження функціональних можливостей навігаційних приймачів студентами. По-перше, кожну секунду вона відображає наступні параметри: широту, довготу, висоту, швидкість, курсовий градус приймача, а також кількість супутників, що приймають участь у вирішенні навігаційної задачі, які відповідно зображено на рис 2. Також можна відобразити різні графіки, наприклад, графік залежності широти або довготи від часу, рівні прийнятих супутникових сигналів, та інші. По-друге, у цьому програмному забезпеченні можливо виконувати багато різних команд керування модулем, таких як:

- Вивчення режимів: «холодного старту» (скидання на заводські установки), «теплого старту» та «гарячого старту»;
- Вивчення роботи приймача при увімкненому та вимкненому режимі супутникової диференційної корекції;
- Вивчення режимів енергоспоживання: неперервний, періодичний, адаптивний та режиму сна (standby);
- Вибір супутникового сузір'я: лише GPS; лише ГЛОНАСС (але без режиму диференційної поправки); GPS та ГЛОНАСС разом.

UTC	SVs	Lat [°]	Lon [°]	Alt [m]	Speed[m/s]	Heading[dgr]
2016-03-26 15:36:35.00	11	50.442848	30.443923	170.80	0.0	0.0
2016-03-26 15:36:36.00	12	50.442848	30.443923	170.80	0.0	0.0
2016-03-26 15:36:37.00	11	50.442848	30.443923	170.80	0.0	0.0
2016-03-26 15:36:38.00	12	50.442848	30.443923	170.80	0.0	0.0
2016-03-26 15:36:39.00	11	50.442848	30.443923	170.80	0.0	0.0
2016-03-26 15:36:40.00	12	50.442848	30.443923	170.80	0.0	0.0
2016-03-26 15:36:41.00	11	50.442848	30.443923	170.80	0.0	0.0
2016-03-26 15:36:42.00	10	50.442848	30.443923	170.80	0.0	0.0
2016-03-26 15:36:43.00	10	50.442848	30.443923	170.80	0.0	0.0
2016-03-26 15:36:44.00	10	50.442848	30.443923	170.80	0.0	0.0
2016-03-26 15:36:45.00	10	50.442848	30.443923	170.80	0.0	0.0
2016-03-26 15:36:46.00	10	50.442848	30.443923	170.80	0.0	0.0
2016-03-26 15:36:47.00	10	50.442848	30.443923	170.80	0.0	0.0
2016-03-26 15:36:48.00	10	50.442848	30.443923	170.80	0.0	0.0

Рис. 2. Кількість супутників, які приймають участь у вирішенні навігаційної задачі, широта, довгота, висота, швидкість, курсовий градус навігаційного приймача через кожну секунду часу.

Але програмне забезпечення Fastrax Workbench має також недоліки:

- не дає можливості розрахунку статистики різних режимів, як, наприклад, програмний засіб SIMCom GPS Demo ver. 3.0;
- у ньому не можна відображати координати на карті Google Maps;
- не можна визначити радіус розкиду визначенних координат та інше.

У результаті дослідження було визначено програмне забезпечення, яке найзручніше буде використовувати в учбовому процесі для вивчення студентами основних параметрів та режимів роботи навігаційних приймачів. Було обрано програмне забезпечення Fastrax Workbench ver. 5 фірми U-blox через його зручний інтерфейс та багатофункціональність.

Література

1. Синякин А.К. Физические принципы работы GPS/ГЛОНАСС/ Синякин А.К., Кошелев А.В. -Новосибирск: СГГА, 2009. –110с.
2. ГЛОНАСС/GPS модуль SIM68V: [Електронний ресурс]. URL: http://mt-system.ru
3. Керамічна пасивна патч-антена фірми AMOTECH: [Електронний ресурс]. URL: http://www.amotech.co.kr.

УДК 621.39

КАНАЛЬНАЯ АДАПТАЦИЯ В СИСТЕМАХ ШИРОКОПОЛОСНОГО РАДИОДОСТУПА IEEE 802.16-2009

Гузовская М.В., Кайденко Н.Н.
Институт телекоммуникационных систем НТУУ «КПИ», Украина
e-mail: m.guzovskaya@gmail.com

Link adaptation in a broadband radio access IEEE 802.16-2009

The IEEE 802.16 technology defines a number of modulation and coding schemes that the base station can use to achieve the best tradeoff between the spectrum efficiency and the resulting application level throughput. Article presents basics of the ARQ and HARQ mechanisms and the adaptive modulation and coding in IEEE 802.16.

Канальная адаптация играет центральную роль в выборе подходящей схемы модуляции и кодирования (MCS), основанной на изменении условий в канале связи, поскольку она значительно улучшает эффективность использования спектра [1], [2], [3]. Система на базе стандарта IEEE 802.16 [4] определяет различные MCS и форматы сообщений для доставки широкополосных услуг.

В этой статье представлены основы механизмов автоматического запроса на повторную передачу (АЗП), гибридного автоматического запроса на повторную передачу (ГАЗП) и адаптивной модуляции и кодирования в системах стандарте IEEE 802.16.

Автоматический запрос на повторную передачу (АЗП) (automatic retransmission request (ARQ)) представляет собой механизм, с помощью которого приемник может запросить повторную передачу пакета данных MAC уровня - MAC PDU (Media access control protocol data unit). Если АЗП включен, для подключения используется расширенная фрагментация подзаголовка (FSH) или расширенная упаковка подзаголовка (PSH) (обозначается расширенный бит в поле типа GMH). Независимо от типа подзаголовка, существует последовательность номера блока (BSN) в подзаголовке, которая указывает на первый номер блока АЗП в PDU. PDU содержит ряд блоков АЗП, каждый из которых имеет постоянный размер, за исключением последнего блока, который может быть меньше. Размер блока АЗП является параметром соединения для отправителя и приемника АЗП после установления соединения. Стоит отметить, что блок АЗП является логическим объектом - границы блоков АЗП не обозначены в явном виде. Остальные номера блоков в PDU можно легко получить, зная размер блока АЗП, общий размер PDU и первый номер блока. По этим причинам именно размер блока АЗП является постоянным параметром. На рис. 1 представлены блоки АЗП с механизмами фрагментации и упаковки. Номера блоков хранятся либо в FSH (см. 1 (а)) или PSH (рис. 1 (б)).

Для того, чтобы запросить повторную передачу блоков (NACK) или для указания успешного приема блоков (ACK), соединение АЗП использует блочную последовательность чисел. В свою очередь, порядковые номера обмениваются сообщениями обратной связи АЗП, зависящих от приёмника.

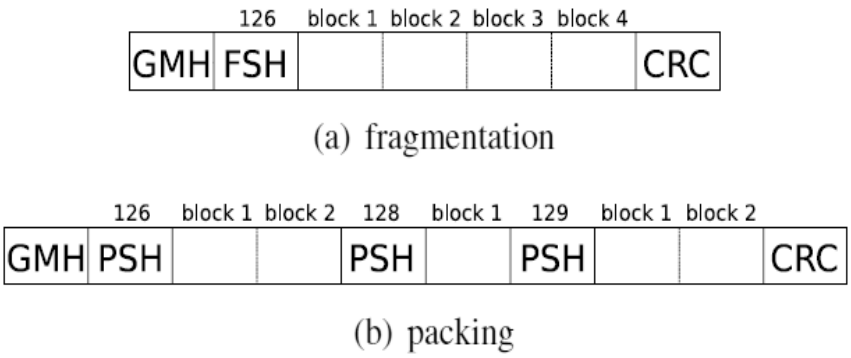


Рис. 1. Структура блоков автоматического запроса на повторную передачу с упаковкой и фрагментацией подзаголовков.

Гибридный АЗП (ГАЗП) (Hybrid ARQ (HARQ)) представляет собой механизм АЗП, который реализуется на физическом уровне вместе с прямой коррекцией ошибок (FEC), обеспечивая улучшенную производительность линии связи по сравнению с традиционными АЗП, за счет повышенной сложности реализации. Простейший вариант ГАЗП представляет собой простое сочетание FEC и АЗП, где блоки данных, наряду с CRC кодом, кодируются с использованием FEC кодера перед передачей; повторная передача запрашивается, если декодер не может правильно декодировать принятый блок. После повторной передачи кодированный блок совмещается с ранее обнаруженным кодированным блоком и подается на вход декодера FEC. Объединение двух полученных версий блока кода повышает вероятность правильного декодирования. Этот тип ГАЗП часто называют тип I или отслеживаемое комбинирование (CC). Наряду со схемой CC, спецификация IEEE 802.16 также определяет режим инкрементальной избыточности (IR), где только дополнительные биты достоверности передаются во время повторной передачи. Вне зависимости от конкретного используемого режима, субпакет ГАЗП имеет обязательное поле CRC-16, как показано на рис. 2. Кроме того, на рисунке показано поле PDU SN, которое служит для аналогичного BSN механизма ARQ.

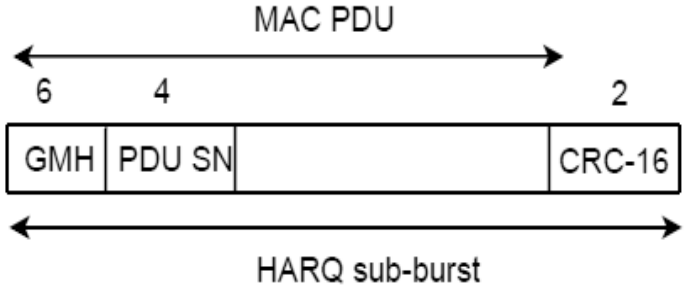


Рис. 2. Структура блока для гибридного автоматического запроса на повторную передачу PDU.

В стандарте IEEE 802.16 поддерживается 16 каналов HARQ наряду с различными поддерживаемыми FEC кодами. Выполнение множества параллельных каналов на ГАЗП может улучшить пропускную способность, поскольку, когда один процесс ГАЗП ждет подтверждения, другой процесс может использовать канал для передачи данных.

Стандарт IEEE 802.16 поддерживает множество схем модуляции и кодирования и позволяет изменять их от пакета к пакету в каждом канале, в зависимости от текущих условий в канале. Используя индикатор обратной связи канала качества, абонентская станция SS может информировать базовую станцию BS о качестве канала нисходящей линии связи. В направлении восходящей линии связи базовая станция может оценивать качество канала на основании принятого качества сигнала. Планировщик BS может принимать во внимание качество каждой восходящей линии связи и канала нисходящей линии связи SS и назначить MCS, который максимизирует пропускную способность исходя из текущего отношения сигнал-шум (SNR). Адаптивная модуляция и кодирование значительно увеличивает общую емкость системы, так как она допускает в режиме реального времени компромисс между пропускной способностью и надежностью.

В направлении нисходящей линии связи QPSK, 16-QAM и 64-QAM, являются обязательными модуляциями, в то время как 64-QAM, не является обязательной в восходящем направлении. FEC кодирование с использованием сверточных кодов является обязательным. Стандарт также опционально поддерживает сверточные (CTC), блочные турбо-коды (BTC), а также коды с низкой плотностью проверки на четность (LDPC) . В общей сложности в [4] определяются 52 комбинации схем модуляции и кодирования в качестве профилей пакетов при использовании CTC, в таблице представлены профили для кодирования с использованием этих кодов. В данной работе мы используем CTC MCS, потому что это единственный блок FEC кодирования, который используется для обоих АЗП и ГАЗП. В таблице представлены блоки FEC и размеры слота этой схемы кодирования.

MCS	*Максимальный размер блока FEC (слот)*	*Размер слота(байт)*
QPSK 1/2	10	6
QPSK 3/4	6	9
16-QAM 1/2	5	12
16-QAM 3/4	3	18
64-QAM 1/2	3	18
64-QAM 2/3	2	24
64-QAM 3/4	2	27
64-QAM 5/6	2	30

Литература

1. J. Hayes. Adaptive feedback communication. IEEE Transactions on Communications, 16(1):29–34, Feb 1968.
2. W.T. Webb and R. Steele. Variable rate MQAM for mobile radio. IEEE Transactions on Comunications, 43(7):2223–2230, Jul 1995.
3. A. Goldsmith and S.-G. Chua. Adaptive coded modulation for fadingchannels. IEEE Transactions on Communication, 46(5):595–602, May 1998.
4. Air interface for fixed broadband wireless access systems – amendment for physical and medium access control layers for combined fixed and mobile operation in licensed bands. IEEE Standard 802.16e, Dec 2005.
5. Air interface for fixed broadband wireless access systems. IEEE Standard 802.16, Jun 2004.

УДК 621.391.17

МАТЕМАТИЧНА МОДЕЛЬ КОГЕРЕНТНОЇ ДЕМОДУЛЯЦІЇ ВЗАЄМНОЗАВАЖАЮЧИХ ЦИФРОВИХ СИГНАЛІВ З МІНІМАЛЬНОЮ ЧАСТОТНОЮ МАНІПУЛЯЦІЄЮ

Єрохін В.Ф., Пелешок Є.В., Захарич О.В.
Інститут спеціального зв'язку та захисту інформації НТУУ «КПІ», Україна
E-mail: pel85@ukr.net

The mathematical model of coherent demodulation mutually interfering digital signals with minimum frequency shift keying

The mathematical model of the compensation procedure of coherent demodulation synchronous mutually interfering digital signals with minimum shift keying is proposed.

При розробці сучасних високоефективних радіозасобів нагальною залишається проблема ефективного використання радіочастотного ресурсу. В реальних умовах прийом радіосигналів здійснюється, як правило, в умовах впливу навмисних або ненавмисних завад, включаючи структурні, що обумовлено обмеженістю радіочастотного ресурсу та зростанням кількості та потужності випромінювань різноманітного походження.

В межах зазначеного актуальним є пошук шляхів повторного використання радіочастотного ресурсу, прийом корисного сигналу в довільній сигнально-завадовій обстановці. На її вирішення спрямована величезна кількість робіт (наприклад, [1,2]).

Пропонується для підвищення завадозахищеності демодуляції корисного цифрового сигналу (ЦС), що спостерігається на фоні потужної структурної завади з метою повторного використання радіочастотного ресурсу застосовувати в приймальних пристроях компенсаційні процедури із застосуванням когерентної (квазікогерентної) демодуляції корисного сигналу та завади [3,4].

Для забезпечення передачі даних в обмеженій смузі частот широко застосовуються цифрові сигнали з мінімальною частотною маніпуляцією (МЧМ). Сигнал з МЧМ може бути представлений як сума двох двійкових взаємно ортогональних попарно протилежних сигналів, оптимальний когерентний прийом якого має завадостійкість навіть дещо вищу, ніж у випадку класичної чотирьохпозиційної фазової маніпуляції [5]. Ширина основної пелюстки спектра потужності сигналу при МЧМ дорівнює $1,5/T$ і майже вся енергія такого сигналу ($\approx 99,9\%$) зосереджена в ньому[12].

Нехай сигнал з МЧМ має індекс маніпуляції, що дорівнює 0,5. На k-му тактовому інтервалі такий сигнал (у загальному випадку сигналів може бути більше одного) представляється наступним виразом [6]:

$$S_i(\hat{r}_{ik}, t) = A_i \cos\left(\omega_0 t + \hat{r}_{ik}\Omega_Д t + \varphi_{ik} + \varphi_{i0}\right),\ t \in [t_{k-1},\ t_k), \qquad (1)$$

де A_i – амплітуда сигналу з МЧМ; $\Omega_Д = \frac{\pi}{2T}$ – девіація частоти; T – тривалість тактового інтервалу; ω_0 – частота несівної; $\hat{r}_{ik} = -(-1)^{r_{ik}}$, $\hat{r}_{ik} = \overline{1,-1}$, $r_{ik} = \overline{0,1}$, $\forall\, i = \overline{1,M}$, $k = 1,2,3...$ – дискретний параметр (ДП); M – кількість синхронних по тактовим точкам сигналів з МЧМ; $\varphi_{ik} = \frac{\pi}{2}\sum_{j=1}^{k-1}\hat{r}_{ij} - \frac{(k-1)\pi}{2}\hat{r}_{ik} = -\frac{\pi}{2}\sum_{j=1}^{k-1}(-1)^{r_{ij}} + \frac{(k-1)\pi}{2}(-1)^{r_{ik}}$ – фаза сигналу на k-му тактовому інтервалі; φ_{i0} – початкова фаза.

З (1) видно, що сигнал з МЧМ залежить від значень інформаційного символу не тільки на k-му тактовому інтервалі, але і від його значень на всіх попередніх інтервалах [1,2]. За два будь-яких сусідніх інтервали фаза сигналу змінюється на $\pm\pi$ або не змінюється, Таким чином, при обробці вхідного спостереження на одному тактовому інтервалі будемо мати справу з демодуляцією ортогональних сигналів, а при обробці на інтервалі $2T$ – протилежних.

Модель вхідного спостереження для випадку, коли в каналі присутні два взаємно синхронних по тактовим точкам МЧМ – сигнали має вигляд:

$$y(t) = -(-1)^{r_1^{п}} S_{11}\left(t \in \left[2kT, 2(k+1)T\right)\right) - (-1)^{r_1^{н}} S_{12}\left(t \in \left[(2k-1)T, (2k+1)T\right)\right) -$$
$$-(-1)^{r_2^{п}} S_{21}\left(t \in \left[2kT, 2(k+1)T\right)\right) - (-1)^{r_2^{н}} S_{22}\left(t \in \left[(2k-1)T, (2k+1)T\right)\right) + n(t), \qquad (2)$$

де $r_1^{п}$, $r_2^{п}$ – ДП на парних тактових інтервалах корисного сигналу та завади відповідно; $r_1^{н}$, $r_2^{н}$ – ДП на непарних тактових інтервалах корисного сигналу та завади відповідно; $S_{11}(t)$, $S_{12}(t)$ – квадратурні складові корисного МЧМ - сигналу, що відповідають значенням його ДП на парних ($\hat{r}_1^{п}$) та непарних ($\hat{r}_1^{н}$) тактових інтервалах відповідно; $S_{21}(t)$, $S_{22}(t)$ – квадратурні складові заважаючого МЧМ - сигналу, що відповідають значенням його ДП на парних ($\hat{r}_2^{п}$) та непарних ($\hat{r}_2^{н}$) тактових інтервалах відповідно; $n(t)$ – адитивний білий гаусівський шум.

В результаті розробки аналітичної моделі когерентної демодуляції синхронних по тактовим точкам взаємнозаважаючих ЦС з МЧМ було отримано правило прийняття рішення про переданий ДП на парних тактових інтервалах корисного сигналу з МЧМ:

$$r_1^{п*} = \operatorname{rect}\left[b_1^{п} - \operatorname{Arth}\left(\operatorname{th} b_2^{п} \operatorname{th} 2R^{п}\right) - \operatorname{Arth}\left(\operatorname{th} b_2^{н1} \operatorname{th} 2R_1^{н}\right) - \operatorname{Arth}\left(\operatorname{th} b_2^{н2} \operatorname{th} 2R_2^{н}\right)\right], \qquad (3)$$

де $b_1^{п} = \frac{2}{N_0}\int_{2kT}^{2(k+1)T} y(t) S_{11}(t)\,\mathrm{d}t$; $b_2^{п} = \frac{2}{N_0}\int_{2kT}^{2(k+1)T} y(t) S_{21}(t)\,\mathrm{d}t$;

$$b_2^{н1} = \frac{2}{N_0}\int_{(2k-1)T}^{(2k+1)T} y(t) S_{22}(t)\,\mathrm{d}t;\ b_2^{н2} = \frac{2}{N_0}\int_{(2k+1)T}^{(2k+3)T} y(t) S_{22}(t)\,\mathrm{d}t;$$

$$R^{\text{п}} = \frac{1}{N_0}\int\limits_{2kT}^{2(k+1)T} S_{11}(t)\,S_{21}(t)\,\mathrm{d}t;\ R_1^{\text{н}} = \frac{1}{N_0}\int\limits_{2kT}^{(2k+1)T} S_{11}(t)\,S_{22}(t)\,\mathrm{d}t;$$

$$R_2^{\text{н}} = \frac{1}{N_0}\int\limits_{(2k+1)T}^{2(k+1)T} S_{11}(t)\,S_{22}(t)\,\mathrm{d}t.$$

Відповідно, правило прийняття рішення про переданий ДП корисного сигналу з МЧМ на непарних тактових інтервалах:

$$r_1^{\text{н}*} = \mathrm{rect}\left[b_1^{\text{н}} - \mathrm{Arth}\left(\mathrm{th}b_2^{\text{н}}\mathrm{th}2R^{\text{н}}\right) - \mathrm{Arth}\left(\mathrm{th}b_2^{\text{п}1}\mathrm{th}2R_1^{\text{п}}\right) - \mathrm{Arth}\left(\mathrm{th}b_2^{\text{п}2}\mathrm{th}2R_2^{\text{п}}\right)\right], \quad (4)$$

де

$$b_1^{\text{н}} = \frac{2}{N_0}\int\limits_{(2k-1)T}^{(2k+1)T} y(t)\,S_{12}(t)\,\mathrm{d}t;\ b_2^{\text{н}} = \frac{2}{N_0}\int\limits_{(2k-1)T}^{(2k+1)T} y(t)\,S_{22}(t)\,\mathrm{d}t;$$

$$b_2^{\text{п}1} = \frac{2}{N_0}\int\limits_{2(k-1)T}^{2kT} y(t)\,S_{21}(t)\,\mathrm{d}t;\ b_2^{\text{п}2} = \frac{2}{N_0}\int\limits_{2kT}^{2(k+1)T} y(t)\,S_{21}(t)\,\mathrm{d}t;$$

$$R^{\text{н}} = \frac{1}{N_0}\int\limits_{(2k-1)T}^{(2k+1)T} S_{12}(t)\,S_{22}(t)\,\mathrm{d}t;\ R_1^{\text{п}} = \frac{1}{N_0}\int\limits_{(2k-1)T}^{2kT} S_{12}(t)\,S_{21}(t)\,\mathrm{d}t;$$

$$R_2^{\text{п}} = \frac{1}{N_0}\int\limits_{2kT}^{(2k+1)T} S_{12}(t)\,S_{21}(t)\,\mathrm{d}t.$$

Синтезована модель може знайти застосування при розробці модемних компенсаторів, що забезпечать повторне використання частотного ресурсу при МЧМ, а також при розробці перспективних завадозахищених засобів радіозв'язку, адаптивних до сигнально-завадової обстановки.

Література

1. Немировский А. С. Метод компенсации помех с использованием частичного частотного разнесения / А. С. Немировский, П. А. Полушин // Электросвязь. – 1990. – № 12. – С. 37–39.
2. Сосулин Ю. Г. Оценочно-корреляционно-компенсационная обработка сигналов на фоне помех / Ю. Г. Сосулин, В. В. Костров // Радиотехника и электроника. – 2006. – Т. 51, № 9. – С. 1027–1065.
3. Бураченко Д. Л. Оптимальное разделение цифровых сигналов многих пользователей в линиях и сетях связи в условиях помех / Д. Л. Бураченко – Л.: ВАС, 1990. – 302 с.
4. Бобровский В. И. Многопользовательское детектирование : Монография / В. И. Бобровский. – У. : Изд-во «Вектор-С», 2007. – 348 с.
5. Аджемов С. С. Перспективы применения частотно-манипулированых сигналов с непрерывной фазой / С. С. Аджемов, Г. Ц. Кастейянос, Н. И. Смирнов // Зарубежная радиоэлектроника. – 1987. – № 9. – С. 3–9.
6. Константинов П. А. Оптимальный прием детерминированных сигналов с минимальной частотной манипуляцией / П. А. Константинов, А. А. Парамонов, Д. Н. Яманов // Изв. вузов МВ и ССО СССР. Радиоэлектроника. – 1983. – Т. 26, № 11. – С. 30–35.

УДК 681.3.06:378.147

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ БЕЗПРОВОДОВИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Примаченко В.І., Сторчак К.П., Макаренко А.О.
Державний університет телекомунікацій, Україна
E-mail: vladuserzvir@ukr.net

Mathematical modelling of wireless telecommunication systems

The article analyzes the process of mathematical modeling of wireless telecommunication systems. Presented methods and tools used in the mathematical modeling of multi-antenna systems using a software environment Matlab Simulink, physical and analytical communication channel.

Одним із суттєвих методів дослідження і удосконалення технологій широкосмугової безпроводової передачі даних є математичне моделювання. Математичне моделювання знаходить найширше застосування в науці, техніці, економіці і освіті [1].

Технологія моделювання складних технічних систем, до класу яких відносяться телекомунікаційні системи, спирається на імітаційне програмне моделювання. Термін “імітаційне моделювання” часто ототожнюється з терміном “статистичне моделювання” [2]. Статистичне моделювання як метод машинної реалізації імітаційних моделей систем, схильних до випадкових дій, - найбільш використовується.

У основі статистичного моделювання лежить процедура, яка використовується для моделювання випадкових величин і функцій - метод статистичних випробувань (метод Монте-Карло).

Загальна схема методу Монте-Карло може бути записана у вигляді [2, 3]

$$M(x) = \int y(x)\, p(x)\, dx. \qquad (1)$$

Результат шукається як математичне очікування деякої випадкової величини y_1, y_2, y_N, яка найчастіше є невипадковою функцією випадкової величини x_1, x_2, x_N, що має розподіл $p(x)$. Наближена оцінка невідомого математичного очікування, співпадаюча з шуканим результатом, знаходиться як середнє арифметичне результатів незалежних дослідів

$$\tilde{M}(x) = \frac{1}{N}\sum_{i=1}^{N} y(x_i),\ x_i \approx p(x). \qquad (2)$$

Результати статистичного моделювання мають випадковий характер, тому для забезпечення статистичної стійкості їхні оцінки визначаються як середнє за великою кількістю реалізацій. Вибір кількості реалізацій визначається вимогами до результатів моделювання. Чим більше реалізацій, тим вища точність моделювання складної системи.

При моделюванні в програмному середовищі Matlab Simulink імітаційна модель схеми має вхідні, вихідні та блоки обробки даних (рис. 1) [4].

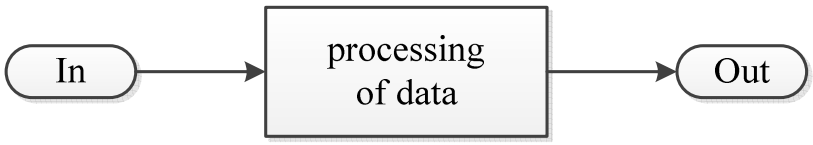


Рис. 1. Структурна схема взаємодії елементів моделі

Алгоритм поведінки моделі системи описується [4, 5]

$$\dot{x}(t) = f(t, x(t), u(t)), \tag{3}$$

де x - вектор стану системи, $x = (x_1, ..., x_n)^T \in R^n$; u - вектор керування, $u = (u_1, ..., u_q)^T \in U \subseteq R^q$, U - деяка задана множина припустимих значень рівняння; t - час, $t \in T = [t_0, t_1]$ - проміжок часу функціонування системи; $f(t, x, u)$ - неперервна разом зі своїми частковими похідними вектор-функції.

На сьогодні бурхливо розвиваються системи ШБД побудовані за стандартами 3GPP LTE, IEEE 802.11 та ін. Ці стандарти об'єднує метод ортогонального частотного мультиплексування (OFDM). З ростом швидкості передачі систем ШБД з'явилась необхідність в розвитку методу Multiple Input Multiple Output (MIMO).

Моделі MIMO-каналу в основному діляться на дві категорії, як показано на рис. 2.

Рис. 2 Моделі поширення каналу MIMO

Фізичні моделі включають в себе як детерміновані, так і стохастичні моделі каналу на геометричній основі [6]:

- детерміновані моделі визначають модель каналу відповідно до передбачення розповсюдження сигналу.

- моделі на геометричній основі мають безпосереднє відношення до фізичних характеристик каналу розповсюдження.

Другий клас моделей MIMO-каналу включає аналітичні моделі, засновані на статистичних властивостях, отриманих за допомогою вимірювань. Аналітичні моделі каналу можуть бути класифіковані як кореляційні моделі (наприклад, модель незалежних однаково розподілених випадкових величин, модель Кронекера, модель Кейхола, ...), статистичні

моделі (наприклад, модель Салех-Валенсуела та модель Цвік) і моделі розповсюдження (наприклад, модель Мюллера та модель повного розсіювання).

Одним із найзначніших удосконалень технології MIMO є багатокористувацька Multiple Input Multiple Output (Multi User - MIMO) технологія. Більшість сучасних комерційних Wi-Fi маршрутизаторів та точок доступу засновані на однокористувацькій технології MIMO (SU-MIMO) або просто MIMO, які використовують неефективні тайм-слотові протоколи для розділення одного повношвидкісного виділеного Wi-Fi з'єднання з декількома клієнтами.

Зазвичай, точки доступу мають 3-4 антени, в той час як більшість клієнтських пристроїв обмежені 1-2 антенами. В такій конфігурації вони не можуть підтримувати повний спектр роботи MIMO-каналу, і повна потужність точки доступу використовується рідко.

Наприклад, точка доступу 802.11ac в режимі 3x3 підтримує пікову швидкість фізичного рівня (PHY) 1.3 Гбіт, але смартфон або планшет з однією антеною підтримує пікову швидкість тільки 433 Мбіт/с, залишивши не використаними 867 Мбіт/с потенціалу точки доступу [6].

MU-MIMO компенсує розрив, дозволяючи точці доступу підтримувати до чотирьох одночасних повношвидкісних Wi-Fi-каналів. Кожен з цих каналів асоційовано з окремим смартфоном, планшетом, ноутбуком, мультимедійним програвачем, або іншим клієнтським пристроєм. В результаті, MU-MIMO дає точці доступу більше варіантів обслуговування своїх клієнтів і дозволяє їй більш ефективно використовувати її загальну ємність, ефективно долаючи MIMO-розрив.

Представлено методи та засоби, які використовуються при математичному моделюванні багатоантенних систем з використанням програмного середовища Matlab Simulink, фізичні і аналітичні моделі каналу зв'язку.

Література

1. Дьяконов В. П. VisSim+Mathcad+MATLAB. Визуальное математическое моделирование. - М.: СОЛОН-Пресс, 2004. - 384 с.

2. Кутузов, О. И., Татарникова Т.М. Моделирование телекоммуникационных сетей. СПб.: [без издательства], 2001. - 76 с.

3. Кривуца В. Г., Барковський В. В., Беркман Л. Н. Математичне моделювання телекомунікаційних систем: Навч. посібник. - К.: Зв'язок, 2007. - 270 с.

4. Лазарєв Ю. Ф. Моделювання динамічних систем у Matlab. Електронний навчальний посібник. – Київ: НТУУ "КПІ", 2011.- 421 с.

5. Алексеев В.М. Оптимальное управление / В. М. Алексеев, В. М. Тихомиров, С. В. Фомин. – М. : Наука, 1979. - 430 с.

6. Almers P. Survey of Channel and Radio Propagation Models for Wireless MIMO Systems [Електронний ресурс] // EURASIP Journal on Wireless Communications and Networking. - Режим доступу: http://publik.tuwien.ac.at/files/pub-et_13071.pdf (01.02.2016.)

УДК 621.396.2

ТЕХНІЧНІ ОСОБЛИВОСТІ ПРОЕКТУВАННЯ БАГАТОКАНАЛЬНИХ СИСТЕМ ДЛЯ ДЕКІЛЬКОХ КОРИСТУВАЧІВ

Макаренко А.О., Гринкевич Г.О., Срочинська Г.С.
Державний університет телекомунікацій, Україна
E-mail: makarenkoa@ukr.net

Technical features of projection of multichannel systems for several users

The work presents an analysis of the prospects for the development of standards IEEE 802.11. It is shown that the 802.11ac specification is one of the most significant technology improvements MIMO. Established that the system antenna circuit four to four and three users are the most productive and efficient for standard 802.11ac.

Технологія MU-MIMO (Multi-User Multiple Input Multiple Output) є спробою вирішення проблеми зростаючого обсягу переданих даних в безпроводових мережах. Завдяки їй, вся пропускна здатність мережі Wi-Fi може бути ефективно використана, а користувачі отримають можливість обміну даними зі швидкістю гігабайт в секунду [1].

З появою пропозицій зі специфікацією 802.11ac значно покращилися радіо-параметри і характеристики нового стандарту.

MU-MIMO спирається на можливість формування променя передачі для встановлення чотирьох одночасних направлених радіочастотних зв'язків. MU-MIMO точка доступу (ТД) використовує розширені методи формування променя для максимізації передачі в напрямку цільового клієнта одночасно зводячи до мінімуму передачу в напрямку небажаних клієнтів через фазово-амплітудну різницю. Цей метод, відомий як метод повторного просторового використання, забезпечує кожного з чотирьох користувачів власним виділеним каналом з повною пропускною здатністю так само, як у стільникових мережах використовують невеликі стільниці і методи повторного використання спектра для збільшення пропускної здатності системи.

У прикладі, показаному на рис. 1, 802.11ac MU-MIMO ТД з чотирма антенами може одночасно передавати кожен просторовий потік на ноутбук, смартфон і планшет окремо [2].

Як і в кожному складному проекті, першим кроком у розробці проекту MU-MIMO є визначення чинників, які мають найбільший вплив на критичні особливості, вартість та продуктивність. Цих чинників є багато, але всі проектні рішення і компроміси опираються на основні два [3]:

- кількість просторових потоків;
- кількість одночасних користувачів.

Кількість просторових потоків. Стандарт 802.11n, що вперше представив MIMO, визначив чотири MIMO потоки як максимально можливу кількість для одночасної передачі одному пристрою. 802.11ac збільшує максимальну

кількість потоків MIMO, отриманих станцією призначення, до восьми, фактично, подвоюючи пропускну здатність мережі 802.11ac у порівнянні з 802.11n.

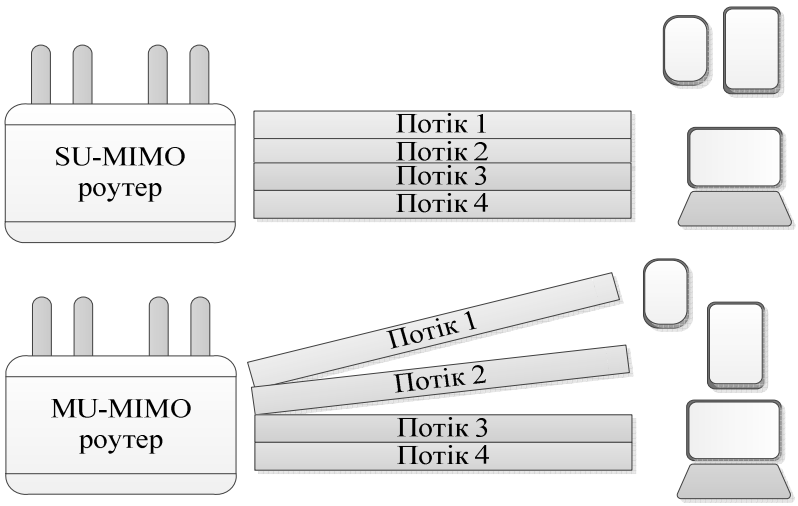


Рис. 1. Принцип дії SU-MIMO і MU-MIMO

Кількість просторових потоків і швидкість передачі разом вказують на потенційну пропускну спроможність і кількість підтримуваних пристроїв. Якщо кожен просторовий потік потребує виділеного каналу прийому/передачі, то ТД стандарту 802.11ac конфігурації 8x8, здатна підтримувати всі вісім просторових потоків, потребує вісім незалежних каналів і антен. Робота на повній потужності ТД стандарту MIMO в конфігурації 8x8 вимагає конфігурації клієнта також 8x8, що є не практично.

Багатьма з пристроїв, які підключаються до Wi-Fi мереж все частіше стають мобільні пристрої, такі як смартфони і планшети, які, як правило, підтримують конфігурацію 1x1 або 2x2. MU-MIMO дозволяє кільком клієнтам розділяти велику кількість потоків ТД.

Кількість одночасних користувачів. 802.11ac MU-MIMO специфікація визначає конфігурацію, що підтримує до чотирьох одночасних MIMO каналів. Додавання можливості підтримки кожного додаткового користувача збільшує загальну вартість рішення. Але, MU-MIMO формування променя вводить кілька інших компромісів, які мають ще більш значний вплив, і, отже, також повинні бути розглянуті до прийняття рішення про кількість підтримуваних користувачів.

Для роботи MU-MIMO, у 802.11ac включено механізми зондування каналу. Кожен клієнт встановлює зворотний зв’язок, де передає інформацію про стан каналу, і ця інформація використовується ТД для застосування необхідних параметрів потужності передачі для кожного просторового потоку. Після того, як канал зондування забезпечує ТД чіткою картинкою про стан його середовища, ТД застосовує механізм формування променя для передачі сигналу в бажаному напрямку і нівелювання передачі сигналу у небажаному напрямку.

На практиці процес формування променя недосконалий, і частина енергії просторового потоку виникає у вигляді бічних пелюсток. Ці дрібні

промені виходять з обох боків від основного променя і направлені на декілька градусів в сторони від вісі основного променя. Хоча це і не є проблемою для SU-MIMO, але два суміжних потоки MU-MIMO починають заважати один одному, як тільки їх бічні пелюстки починають перекриватися. Наявність цього втручання створює додатковий шум каналу.

Число одночасно підтримуваних користувачів ТД сильно впливає на підходи по проектуванню систем MU-MIMO. Додавання четвертого просторового MU-потоку додає міжпотокову інтерференцію, але збільшує кількість доступних просторових потоків. Так що є компроміс. Яке рішення забезпечує кращу пропускну здатність мережі? Це залежить від навколишнього середовища каналу багатопроменевого розповсюдження. Багатопроменеві характеристики внутрішнього каналу визначають скільки перешкод створюється при додаванні ще одного MU-потоку. Досить завантажене середовище підтримує до трьох просторових потоків з допустимою інтерференцією, забезпечуючи при цьому найвищий рівень роботи схеми модуляції та кодування. При додаванні четвертого потоку, інтерференція перешкоджає роботі найвищих рівнів модуляції та кодування, і, таким чином, пропускна здатність знижується.

При проектуванні систем MU-MIMO необхідно дотримуватись наступних важливих висновків [3]:

- система в конфігурації 4 на 4 з трьома користувачами досягає максимальної продуктивності і стабільності роботи MU-MIMO. ТД з 4 антенами і 3-ма користувачами N+1 дає можливість MU-MIMO методу формування променя набагато ширший діапазон руху шляхом зменшення інтерференції і підвищення загальної пропускної спроможності каналу.

- ТД такої конфігурації забезпечує повноцінну роботу MU-MIMO для підтримки високої пропускної здатності низхідної лінії зв’язку і підвищує дальність дії для більш простих (не MIMO) клієнтів.

- за багатьох умов, додавання четвертого користувача значно зменшує доступну пропускну спроможність системи, продуктивність і швидкість передачі.

Висновки. 802.11ac з MU-MIMO призначений для забезпечення потужності і продуктивності, необхідної для підтримки сучасних пристроїв та додатків, і відкриває нові можливості для майбутніх додатків. Але його широке поширення і впровадження залежить від наявності 802.11ac рішень з MU-MIMO, які забезпечать усі переваги технології в порівнянні з обладнанням попереднього покоління 802.11n.

Література

1. MU-MIMO - революция в Wi-Fi [Електронний ресурс] // – Режим доступу: http://itbusiness.com.ua/hardnews/1315-mu-mimo-revolyutsiya-v-wi-fi.html (02.03.2016.)
2. Difference between single user MIMO vs Multiuser MIMO [Електронний ресурс] // – Режим доступу: http://www.rfwireless-world.com/Terminology/single-user-MIMO-vs-multiuser-MIMO.html (02.03.2016.)
3. 802.11ac MU-MIMO: Bridging the MIMO Gap in Wi-Fi / Qualcomm Atheros Inc. – January, 2015. - 14 p.

УДК 621.396

МЕТОД НАВЧАННЯ БАЗИ ЗНАНЬ ПІДСИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МОБІЛЬНОЇ РАДІОМЕРЕЖІ КЛАСУ MANET НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ ТА АПАРАТУ НЕЙРОННИХ МЕРЕЖ

Сальник С.В., Сальник В.В., Лукіна К.В.
Військовий інститут телекомунікацій та інформатизації, Київ, Україна
E-mail: sergey.00@rambler.ru

A method studies of bases knowledge subsystem providing security of mobile radio networks class MANET is on basis of fuzzy logic and apparatus neural networks

A purpose in the article and features of security providing subsystems using in process of management the MANET and functioning is considered. The found out actuality development methods studies of bases knowledge subsystem providing security. Offered method realization studies of bases knowledge is base on that complex application neuro-fuzzy logic

Організація ефективного управління мобільними радіомережами (МР), що відносяться до класу MANET (Mobile Ad-Hoc Networks) потребує вирішення множини завдань, одним з яких є забезпечення безпеки передачі інформаційних даних. Зважаючи на особливості функціонування МР, такі як складність побудови, динамічна природа функціонування, децентралізованість, та масштабованість, призводить до необхідності реалізації підсистеми забезпечення безпеки (ПЗБ), робота якої потребує застосування спеціалізованого обладнання, алгоритмів та методів [1].

З метою забезпечення безпеки передачі даних в МР, зумовленою необхідністю обробки значних об`ємів службової інформації про стан об`єктів управління, в якості яких може виступати, як мобільний вузол так і параметри інформаційного обміну, в основі ПЗБ повинна бути покладена система знань. Вона повинна використовувати мову подання знань, яка б надавала можливості адекватно відтворювати структуру об’єктів управління і характеризувалася достатньою формальністю та логічністю. Саме це дозволить побудувати компактну, строгу та чітку систему знань з можливістю самонавчання.

Функціонування будь-якої ПЗБ ґрунтується на перетворенні інформації в знання, на основі яких будуть прийматися управлінські рішення. ПЗБ у результаті збору та обробки інформації отримує знання про стан мережі, інших вузлів та ситуацію, що склалася в МР. Ці знання являють собою сукупність відомостей про кожен компонент МР, а також множину правил використання цієї інформації для прийняття управлінських рішень в МР. На практиці оперування знаннями в ПЗБ здійснюється базою знань (БЗ). У зв’язку з вказаним, актуальним є питання розробки підходів щодо навчання БЗ у ПЗБ.

БЗ являє собою особливого роду базу даних, яка містить структуровану інформацію, котра використовується функціональними підсистемами вузла для прийняття управлінських рішень на різних рівнях моделі OSI. За способом навчання методи отримання знань поділяються на: навчання з учителем, де для кожного прецеденту примусово задається пара „ситуація – необхідне рішення”; навчання без учителя – спосіб машинного навчання, під час якого досліджувана

система навчається виконувати завдання, без втручання з боку експериментатора. Як правило даний спосіб навчання придатний для завдань, в яких відомі описи множин об’єктів, і необхідно виявити внутрішні взаємозв’язки, залежності та закономірності, що існують між об’єктами [2].

Виходячи з вказаного, для ПЗБ доцільно використовувати методи навчання з учителем на етапі побудови мережі, а для самонавчання мережі необхідно використовувати методи без учителя, основною рисою яких є здатність до самоорганізації. Вирішенню питань самонавчання БЗ присвячені роботи Д.О. Хебба, А.П. Карпенко, В.В. Борисова. Однак, в основному ці роботи не враховують особливостей функціонування МР. У зв’язку з цим пропонується підхід самонавчання БЗ, який дозволить здійснювати поповнення новими знаннями БЗ вузлової ПЗБ за допомогою застосування нейро-нечіткої логіки.

Нейронні мережі (НМ) мають здатність проводити навчання, в наслідок якого НМ спроможна виявляти складні залежності між вхідними та вихідними даними, а також проводити кластеризацію вхідних образів. Нечітка логіка (НЛ), базується на нечітких множинах та дозволяє здійснювати математичну формалізацію логіко-лінгвістичної інформації, яка застосовується при описі складних нелінійних об'єктів. Як правило, моделювання таких об'єктів зводиться до побудови БЗ, які втілюють в собі експертні знання про об'єкт у вигляді лінгвістичних висловлювань ЯКЩО-ТО, що відноситься до переваг [3].

Метод навчання ПЗБ враховуючи особливості функціонування МР повинен проводити збір даних на основі проведення самонавчання, тому запропонований метод повинен мати таки властивості як: навчання без учителя; рішення задач класифікації та кластеризації даних; прогнозування, адаптація мережі для роботи при нечіткій мережевій активності; наявність обернених зв’язків; проведення навчання в режимі реального часу. Як показав проведений аналіз для побудови баз знань ПЗБ за основу доцільно обрати метод навчання Хебба [4], а метод буде складатися з наступних кроків:

Так як метод навчання баз знань ПЗБ полягає в обчислення попередніх вимірів виходів для визначення змін ваг, то для навчання БЗ буде використано диференційний метод, що

1. Ініціалізація, де всім ваговим коефіцієнтам присвоюються випадкові значення. При формуванні бази правил з урахуванням не прогнозованих процесів у МР, при випадкових впливах та в умовах динамічності та нечіткості необхідно використовувати апарат нечітких множин та НМ.

На підставі аналізу предметної області, особливостей застосування нейро-нечітких мереж, характеристичних особливостей МР та вимог до методу навчання БЗ, доцільно обрати нечітку нейронну мережу Такагі-Сугено-Канга, яка забезпечить найменшу похибку навчання та найкращу точність прогнозування [5].

2. Реалізація нечіткого виводу вузловою ІСУ, який здійснюється відповідно до наступних етапів [6]:

– фазифікація, яка полягає у встановленні відповідності між конкретним значенням окремої вхідної змінної системи нечіткого виводу і значенням, яке відображає ступінь істинності підумови правила на основі значення функції належності відповідного їй терма вхідної лінгвістичної змінної;

– агрегування, де відбувається визначення ступеню істинності умов за кожним з правил системи нечіткого виводу на основі відомих значень істинності підумов, які входять до нього;

– активація, яка передбачає визначення значень функції належності кожного з підвисновків для вихідних лінгвістичних змінних, які розглядаються;

– акумулювання, яке передбачає об'єднання і акумулювання з використанням операції max-диз'юнкції всіх ступенів істинності підвисновків для отримання функції належності кожної із вихідних змінних;

– дефазифікація, яка полягає в отриманні чітких (кількісних) значеннях кожної із вихідних змінних, які можуть бути використані підсистемами вузла в процесі його функціонування.

3. На входи мережі подається вхідний образ, а сигнали збудження розповсюджуються по всім шарам відповідно принципів класичних прямопотокових мереж [7], тобто для кожного нейрону розраховується зважена сума його входів, до якої застосовується активаційна (передаточна) функція нейрону, в результаті чого отримуємо його вихідне значення.

4. Проведення навчання НМ з співвідношенням швидкості навчання та налаштуванням ваг до значень параметрів швидкості навчання [8].

5. На основі отриманих вихідних значень нейронів здійснюється зміна вагових коефіцієнтів.

6. Перевірка відповідності вхідних значень до висунутих вимог.

Таким чином, було запропоновано метод навчання БЗ підсистеми забезпечення безпеки МР класу MANET при комплексному використанні нечіткої логіки та апарату НМ.

Література

1. Машинное обучение [электронный ресурс] // Матеріал з Вікіпедії. – Останнє оновлення сторінки 14.01.2015. – Режим доступу: https://ru.wikipedia.org/wiki/Машинное_обучение.
2. Комашинский В.И. Нейронные сети и их применение в системах управления и связи // Комашинский В.И., Смирнов Д.А. – М.: Горячая линия–Телеком, 2002. – 94 с.
3. Стариков А. Нейронные сети – математический аппарат [электронный ресурс] // Стариков А. – Base Group Labs. – Режим доступа: http://www.basegroup.ru/library/analysis/neural/math.
4. Зайченко Ю.П. Нечеткие модели и методи в интеллектуальних системах.-К., „Слово", 2008. – 344 с.
5. Штовба С.Д. Введение в теорию нечетких множеств и нечеткую логику // Штовба С.Д. – Винница: Континент-Прим. – 2003. – 198 с.
6. Искусственный интеллект и интеллектуальные системы управления // И.М. Макаров, В.М. Лохин, С.В. Манько, М.П. Романов.– М.: Наука, 2006. – 333 с.
7. Lakshmi C.J. Fusion of Neural Networks, Fuzzy Systems and Genetic Algorithms: Industrial Applications // Lakshmi C.J., Martin N.M. – CRC Press, 1998. – 368 p.
8. Рутковская Д. Нейронные сети, генетические алгоритмы и нечеткие системы // Рутковская Д., Пилиньский М., Рутковский Л. – 2-е изд. – М: Горячая линия-Телеком, 2008. – 452 с.

УДК 621.396

МЕТОДИКА ВИБОРУ РОБОЧИХ ЧАСТОТ ДЛЯ СИСТЕМ РАДІОЗВ'ЯЗКУ З ПСЕВДОВИПАДКОВОЮ ПЕРЕСТРОЙКОЮ РОБОЧОЇ ЧАСТОТИ

Кувшинов О.В., Борознюк М.В., Рубцов І.Ю.
Військовий інститут телекомунікацій та інформатизації, Україна
E-mail: igor@rubtsov.com.ua

High order modes of dielectric resonator for microwave applications

The report provides the backup method of choice for radio frequencies with adaptive frequency hopping. The concepts of vector frequency, time, steady-state operation of the radio link. Based on the definition of these indicators are designed to the requirements of the operating frequencies. The proposed method can be used in the design of anti-interference of decameter communication systems.

Одним з ефективних режимів роботи засобів радіозв'язку, що забезпечує необхідний рівень завадозахищеності ліній декаметрового зв'язку, є режим адаптивної програмної перестройки робочої частоти (ППРЧ).

Його практична реалізація передбачає вибір робочих частот, рівень шуму на кожній з яких не перевищує допустимого значення. В загальному випадку це є нетривіальною задачею, тому для її рішення пропонується наступна методика.

Визначення часу стійкого стану в радіолінії з ППРЧ. Під режимом адаптивної ППРЧ будемо вважати режим програмної перебудови, при якому для функціонування радіолінії обираються частоти, на яких забезпечуються найкращі умови зв'язку по показнику достовірності.

Для оцінки ступеня нерівномірності вибору робочих частот радіолінії введемо поняття коефіцієнту використання *i*-тої частоти як відношення сумарного часу роботи на зазначеній частоті$\left(\tau_{\sum_i}\right)$ до загального часу функціонування в режимі ППРЧ (T_a):

$$\alpha_i = \tau \sum\nolimits_i / T_a . \qquad (1)$$

де $T_a = \sum_{i=1}^{m} \tau_{\sum_i}$, i=1,2,…, m; m – число частот, що виділені для функціонування радіолінії.

Сукупність значень $\{\alpha_i\}$ утворюють вектор робочих частот $A = \|\alpha_1, \alpha_2 ... \alpha_m\|$, який визначимо як функцію часу:

$$A(t) = \|\alpha_1(t), \alpha_2(t) ... \alpha_m(t)\| . \qquad (2)$$

З урахуванням виразу (2) введемо поняття часу стійкого стану як значення часу інваріантного вектору $A(t)=\|\alpha_1(t),\alpha_2(t)...\alpha_m(t)\|$, яку буде визначатися ефективністю функціонування радіолінії з адаптивною ППРЧ.

Для аналітичного представлення введеного поняття припустимо, що радіолінія функціонує в умовах навмисних завад, що представлені у вигляді адитивного білого гаусівського шуму коли перевищення рівня сигналу над рівнем завад $z_i = y_i - x_i$ на кожній з робочих частот описується стаціонарною кореляційною функцією вигляду [1]

$$B_i(\tau)=\exp\left(-\tau^2/2\tau_{z_i}^2\right),. \qquad (3)$$

де τ_{z_i} - інтервал кореляції рівня сигналу на *i*-тій частоті; *i*= 1,2,..., *m*.

Припустимо також, що зміна значення коефіцієнту використання *i*-тої частоти відбувається при пересіченні амплітуди випадкового процесу $z_i(t)$ допустимого значення перевищення рівня сигналу над рівнем завад $z_{\text{доп}}$.

Для розглянутих умов час стійкого стану для радіолінії з адаптивною ППРЧ $\bar{\tau}_{\text{стійк}}$ ППРЧ визначимо як мінімальний інтервал пересічення випадковим процесом $z_i(t)$ рівня $z_{\text{доп}}$. Тоді середню тривалість позитивного $\bar{\tau}_{\text{пр}i}$ та негативного $\bar{\tau}_{\text{непр}\,i}$ викидів процесу з параметрами

$\bar{z}_i, \delta_{zi}, B_i(\tau)\ (i=1,2,...,m)$ розрахуємо з використанням виразів з [1]:

$$\bar{\tau}_{\text{пр}i}=\frac{2\pi}{\sqrt{-B''_{0i}}}\left(1-F\left(\frac{z_{\text{доп}}-\bar{z}_i}{\delta_{z_i}}\right)\right)\exp\left(\left(z_{\text{доп}}-\bar{z}_i\right)^2/2\delta^2{}_{z_i}\right); \qquad (4)$$

$$\bar{\tau}_{\text{непр}i}=\frac{2\pi}{\sqrt{-B''_{0i}}}F\left(\frac{z_{\text{доп}}-\bar{z}_i}{\delta_{z_i}}\right)\exp\left(\left(z_{\text{доп}}-\bar{z}_i\right)^2/2\delta^2{}_{z_i}\right); \qquad (5)$$

де $F(\varepsilon)=\frac{1}{2\pi}\int_{-\infty}^{\varepsilon}e^{\frac{t^2}{2}}dt$ - інтеграл ймовірності Лапласа [1];

$B''_{0i}=\left(\frac{\delta_{x_i}}{\delta_{x_i}+\delta_{y_i}}\frac{1}{\tau_{x_i}^2}+\frac{\delta_{y_i}}{\delta_{x_i}+\delta_{y_i}}\frac{1}{\tau_{y_i}^2}\right)$ - друга похідна від функції кореляції при нульовому значенні аргументу; $\delta_{z_i}=\sqrt{\delta_{x_i}^2+\delta_{y_i}^2}$ - середньоквадратичне відхилення перевищення рівня сигналу над рівень завад.

Введемо поняття стійкого стану *i*-тої робочої частоти $\bar{\tau}_{\text{стійк}\,i}$, під яким будемо розуміти математичне очікування інтервалу часу, на протязі якого будемо розуміти $z_i(t)\geq z_{\text{доп}}$ або $z_i(t)< z_{\text{доп}}$:

$$\overline{\tau}_{\text{стійк } i} = P_i\left(P_{\text{пом}} \le P_{\text{пом } i}\right)\overline{\tau}_{\text{пр } i} + \left(1 - P_i\left(P_{\text{пом}} \le P_{\text{пом } i}\right)\right)\overline{\tau}_{\text{непр } i}, \quad (6)$$

де $P_i\left(P_{\text{пом}} \le P_{\text{пом}i}\right) = F\left(\dfrac{\overline{z}_i - \overline{z}_{\text{доп}}}{\delta_{z_i}}\right) = \dfrac{\overline{\tau}_{\text{пр}i}}{\overline{\tau}_{\text{пр}i} + \overline{\tau}_{\text{непр}i}}$ [2].

З урахуванням введених визначень та обмежень час стійкого стану в адаптивній радіолінії з ППРЧ представимо як:

$$\overline{\tau}_{\text{стійк ППРЧ}} = \min\left\{\overline{\tau}_{\text{стійк } i}\right\}. \quad (7)$$

Вираз (6) перетворимо до вигляду:

$$\overline{\tau}_{\text{стійк ППРЧ}} = \min\left\{\frac{2\pi}{\sqrt{-B''_{0i}}}\exp\left(\left(z_{\text{доп}} - \overline{z}_i\right)^2 / 2\delta^2_{z_i}\right)\left[\left[1 - F\left(\frac{z_{\text{доп}} - \overline{z}_i}{\delta_{z_i}}\right)\right]^2 + F^2\left(\left(z_{\text{доп}} - \overline{z}_i\right) / \delta^2_{z_i}\right)\right]\right\} \quad (8)$$

.

Висновки:

З аналізу отриманих результатів можна сказати, що вибір резервних частот для радіолінії з адаптивною ППРЧ необхідно проводити з урахуванням параметрів випадкового процесу перевищення рівня сигналу над рівнем завад на зазначених частотах.

Основні етапи методики вибору резервних частот для радіолінії х адаптивною ППРЧ визначимо наступні:

- для кожної з робочих частот визначається середньоквадратичне відхилення рівня завад, інтервали кореляції завад, рівень сигнал/завада;

- ранжуються робочі частоти по критерію найбільшого значення рівня і інтервалу кореляції завад, перевищення середнього рівня сигналу над середнім рівнем завад близького до допустимого значення;

- визначення часу стійкого стану для кожної з частот;

- ранжуються частоти по часу стійкого стану;

- здійснення вибору робочих частот.

Запропонована методика може бути при проектуванні завадостійких систем військового радіозв'язку.

Література

1. Адаптивные автоматизированные системы военной радиосвязи / Ю.П. Килимник, Е.В. Лебединский, В.К. Прохоров, А.Н. Шаров; Под ред. А.Н. Шарова.-Л.: ВАС, 1978.-284 с.
2. Военные системы радиосвязи. Часть II / Под ред. В.В. Игнатова.- Л.: ВАС,1990 - 176 с.

УДК 621.382

ОЦІНКИ ЙМОВІРНОСТІ ПРАВИЛЬНОГО ВИЯВЛЕННЯ СИГНАЛІВ З РАЙСОВСЬКИМИ ЗАВМИРАННЯМИ

Руденко Д.М.
Військовий інститут телекомунікацій та інформатизації , Україна
E-mail: rudenko1980@meta.ua

Estimating the probability of correct detection of signals with Rician fading

The method for obtaining an analytic expression for the probability of correct detection of incoherent signal processing circuit exposed Rician fading.

Більшість завдань теорії виявлення сигналів на тлі гауссовских шумів вирішені для випадків прийому сигналів з флуктуючою початковою фазою або з флуктуючою початковою фазою і амплітудою (тобто завмираннями), розподіленої по релеевскому закону. Для таких сигналів оптимальною буде структурна схема приймача некогерентного виявлення. У додатку до цієї схеми отримані функціональні залежності (φ) ймовірності правильного виявлення (D) сигналів від ймовірності помилкової тривоги (F) і відносини енергії сигналу до спектральної щільності шуму (E_r/N_0) для двох випадків: 1) приймання сигналів з флуктуючою фазою $D=\varphi_1(E_r/N_0,F)$; 2) прийому сигналів з флуктуючою фазою і релеевскому завмираннями амплітуди $D=\varphi_2(E_r/N_0,F)$.

Однак в загальному випадку амплітуда сигналів може мати райсовський (узагальнений релеевський) розподіл. Цей розподіл характеризується параметром Райса γ^2, який може приймати значення від $\gamma^2=0$ (при релеевському завмиранні) до $\gamma^2=\infty$ (при відсутності завмирань).

В даний час відомо лише одна формула для оцінки залежності $D=\varphi_3\left(E_r/N_0,F,\gamma^2\right)$ ймовірності правильного виявлення сигналів від відносини сигнал/шум, ймовірності помилкової тривоги і параметра Райса. Однак достовірність цієї формули викликає сумніву, оскільки вона не зводиться в окремих випадках (тобто $\gamma^2=\infty$ і $\gamma^2=0$) до відомих залежностей

$D = \varphi_1(E_r/N_0, F)$ та $D = \varphi_2(E_r/N_0, F)$ при відсутності зауважень та їх релеевский характер.

Дослідження показали, що в некоррельованому релеєвському MIMO-каналі можна збільшити пропускну здатність в *n* разів (де *n* – мінімум з числа передавальних і приймальних антен) порівняно з системою з одним входом і одним виходом (SISO : *Single Input – Single Output*) при такому ж відношенні сигнал-шум. Модель релеєвського каналу без урахування просторової кореляції, яка погіршує пропускну здатність, не завжди адекватна реальному каналу. Антенна (або просторова) кореляція притаманна каналам з розсіюванням і залежить від відстані між передавальними і приймальними антенами, а також від відстані між антенними елементами та їх конфігурації .

З математичної точки зору оцінка пропускної здатності MIMO-систем в каналах із завмираннями зводиться до усереднення наведеної до смуги частот миттєвої Шеннонівської пропускної здатності з розподілу комплексної матриці каналу або сформованої на її основі комплексної матриці Уішарта. Матриця Уішарта в залежності від виду завмирань має центральний (в релеєвському каналі) і нецентральний (в райсовському каналі) розподіл Уішарта. Шляхом нескладних перетворень усереднення по розподілу Уішарта можна звести до усереднення по розподілу власних значень матриці Уішарта. Однак незважаючи на те, що починаючи з робіт Уішарта багато дослідників приділяли велику увагу цьому завданню (отримання розподілу власних значень), воно не знайшло ще свого остаточного рішення в загальному вигляді для нецентрального (в райсовскому каналі) розподілу.

Таким чином, виникає необхідність розробити методику отримання аналітичного виразу для оцінки ймовірності правильного виявлення сигналів з райсовскими завмираннями з некогерентного схемою їх обробки в залежності від параметра глибини завмирань, яке в окремих випадках зводиться до відомим виразами для некогерентного виявлення сигналів з випадковою початковою фазою і сигналів з випадковою початковою фазою і релеевскими завмираннями.

УДК 621.391

ОЦЕНКА ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ ИНТЕЛЛЕКТУАЛЬНЫМИ УСЛУГАМИ

Пустовой Б. Л., Кунуп Т.В.
Институт холода, криотехнологий и экоэнергетики им. В. С. Мартыновского Одесской национальной академии пищевых технологий, Украина
E-mail: b.pustoviy@gmail.com

Appreciation of the efficiency of management of intellectual services

The paper discusses the criterions of appreciation of the efficiency of management of intellectual services. The criterions were not considered earlier. It was offered the methods of comparison of different management principles.

В связи с возросшим спросом на современные интеллектуальные услуги возникает необходимость в повышении эффективности управления предоставляемыми услугами. Эффективность управления интеллектуальными услугами зависит от возможности обеспечить оптимальные значения критериев качества обслуживания заявок на интеллектуальные услуги. Исходя из этого, задача определения эффективности управления интеллектуальными услугами является актуальной.

Оценка эффективности управления интеллектуальными услугами связана с анализом архитектуры сети, принципом построения системы управления и разработкой результирующего критерия эффективности управления интеллектуальными услугами.

Вопросы, связанные с исследованием методов оценки эффективности управления интеллектуальными услугами, рассмотрены в работах В.К. Стеклова, Л.Н. Беркман [1], Н.О. Князевой [2], Е. Штейнберга, С.В. Шестопалова [3]. В работах [2, 3] устройства управления рассмотрены как система массового обслуживания – СМО (при централизованном принципе управления) или как сеть массового обслуживания – СеМО (при децентрализованном или смешанном принципах управления). Поступающие потоки заявок на обслуживание считаются пуассоновскими. В результате использования этих моделей полученные характеристики СМО (СеМО) оказываются более оптимистичными, чем характеристики реальных сетей.

В работах [4–6] показано, что сетевой трафик обладает ярко выраженными свойствами самоподобия. Учет этих свойств позволяет более точно характеризовать поведение сетевого трафика, нежели при использовании пуассоновских моделей.

Параметром, характеризующим степень самоподобия, является параметр Херста H, $0 < H < 1$, определяемый для временного ряда $x(t_i)$, t_i –

дискретные моменты времени, $1 \le i \le N$ [5]. Если $H > 0{,}5$, то исследуемый поток обладает длительной памятью и является самоподобным [4].

Исходя из результатов работ [4–6], определена необходимость при оценке эффективности управления интеллектуальными услугами учитывать свойство самоподобия поступающих потоков заявок на обслуживание.

В работах по оценке эффективности управления интеллектуальными услугами [1–3] преимущественно рассматриваются технические характеристики, в соответствии с требованиями к сетевым показателям качества для служб, основанных на протоколе IP [7]. Однако, исходя из современных рекомендаций МСЭ [8], при оценке телекоммуникационного сервиса необходимо учитывать степень удовлетворенности пользователей качеством сервиса.

При формировании оценки (критерия) эффективности управления интеллектуальными услугами в данной работе, на основании проведенных исследований, предложены следующие составляющие (подкритерии) критерия эффективности управления интеллектуальными услугами:

1. Технические подкритерии: общее время обслуживания заявки на интеллектуальную услугу T, вероятность блокировки заявки P, количество заявок, которые ожидают обслуживания L.

2. Экономический подкритерий – общая стоимость устройства управления (при соответствующем принципе управления) – C.

3. Подкритерий, учитывающий характер поступающего потока заявок на обслуживание – H.

4. Подкритерий, характеризующий степень удовлетворенности пользователей качеством сервиса – $П$.

Критерий Q эффективности управления интеллектуальными услугами представляется в векторной форме:

$$\bar{Q} = (T, P, L, C, \text{Н}, \text{П}). \quad (1)$$

При сравнении эффективности устройств управления с различными принципами управления на основе векторного критерия в форме (1) необходимо, чтобы все подкритерии устройства управления с определенным принципом управления соответствовали аналогичным подкритериям устройства управления с другим принципом управления. Если же данное условие не выполняется, то необходимо вводить дополнительные условия для сравнения эффективности устройств управления с различными принципами управления. Однако, не всегда возможно сравнить устройства управления с разными принципами управления с помощью вектора, элементами которого являются подкритерии. Чаще всего сначала формируется векторный критерий, а затем осуществляется переход к результирующему скалярному критерию методами, представляющими

возможность количественной оценки эффективности управления интеллектуальными услугами [3].

Для его создания используется аддитивная функция полезности:

$$Q(x)=\sum_{k=1}^{S}\lambda_k Q_k(x),\ \lambda_k \geq 0,\quad \sum_{k=1}^{S}\lambda_k=1\ , \qquad (2)$$

где Q_k – значение k-го подкритерия, выставляется в баллах в принятой системе оценок; λ_k – весовой коэффициент, определяющий значимость k-го подкритерия; S – количество подкритериев.

Для определения значений весовых коэффициентов подкритериев обычно используются экспертные оценки, на основании которых формируется матрица приоритетов [1].

Сравнение полученных результатов – значения критерия Q для устройств управления с различными принципами управления – позволяет выполнить оценку эффективности управления интеллектуальными услугами.

Современные требования к эффективности управления интеллектуальными услугами делают необходимым введение дополнительных характеристик при выборе принципа управления интеллектуальными услугами. В данной работе наряду с техническими и экономическими подкритериями, предложены подкритерии учета мнения пользователей и самоподобия трафика, которые позволяют более точно оценить эффективность работы устройства управления интеллектуальными услугами с различными принципами управления.

Литература

1. Проектування телекомунікаційних мереж / [В.К. Стеклов, Л.Н. Беркман]. – Техніка, 2002. – 792 с.
2. Князєва Н.О. Підвищення якості управління послугами при застосуванні децентралізованої системи управління /Н.О. Князєва, С.В. Шестопалов // Вісник ДУІКТ. – т.8. – №1 – К.: ДУІКТ, 2010р. – С. 21-28.
3. Шестопалов С.В. Качество управления интеллектуальными услугами в сетях последующего поколения // International Journal «Information Models and Analyses» Vol.2/2013, Number 3. – 2013. – с.262-274
4. Ладыженский Ю.В., Моргайлов Д.Д., Моатаз Юнис. Моделирование самоподобного входного трафика сетевых процессоров в системе NS-2 // Наукові праці ДонНТУ випуск 16 (204) Серія “Інформатика, кібернетика 2012 та обчислювальна техніка”
5. Кириченко Л.О., Чалая Л.Э. Комплексный подход к исследованию фрактальных временных рядов // International Journal “INFORMATION TECHNOLOGIES & KNOWLEDGE”. - 2014. - Vol.8., №1. - С.22-28
6. Цыбаков Б.С. Модель телетрафика на основе самоподобного случайного процесса // Радиотехника. 1999. - № 5. - С. 24-31.
7. Требования к сетевым показателям качества для служб, основанных на протоколе IP: МСЭ-Т. – Y.1541. – [Переизд. Фев. 2007 с изм.]. – Женева, 2007. – 43 с.
8. “Международный союз электросвязи (ITU)”, официальное Интернет-представительство. — Режим доступа: http://www.itu.int (дата обращения 20.03.2015 г.).

УДК 621.396

МЕТОД РОЗМІЩЕННЯ БАЗОВИХ СТАНЦІЙ В МЕРЕЖАХ МОБІЛЬНОГО ЗВ'ЯЗКУ П'ЯТОГО ПОКОЛІННЯ

Гуськов П.О., Бак Р.І.
Національний університет «Львівська політехніка», Україна
E-mail: p.huskov@gmail.com, bak_roman@yahoo.com

The Method of Base Stations Allocation in 5G Mobile Networks

The method of radio access network structure optimization that aims to support different subscribers spacial distribution is represented. It's shown that according to current load conditions partial BS excluding doesn't cause additional depravation of quality parameters.

Для мобільних мережі п'ятого покоління характерне використання частот в міліметровому діапазоні та щільне розташування базових станцій. Дослідження показують, що 80% користувачів концентруються на 20% радіопокриття. Відповідно, доцільним є впровадження малих комірок, оскільки розміщення базових станцій ближче до користувача знижує наскрізну (end-to-end) затримку та підвищує кількість доступних ресурсів для окремого користувача [1].

Використання малих комірок дозволить проводити оптимізацію радіопокриття. При цьому основним завданням є мінімізація кількості макро- і мікро- БС (базові станції) в мережі при задоволенні наступних обмежень:

1) Для усіх користувачів повинні задовольнятись вимоги по SINR.

2) Всі користувачі повинні отримувати потужність сигналу, що перевищує заданий пороговий рівень.

3) Користувач *k* може обслуговуватись БС *i*, тільки якщо БС *i* є активною в даний момент.

4) Кожен користувач може обслуговуватись як мінімум однією БС.

5) Кожна БС може обслуговувати певну кількість користувачів на основі доступних піднесучих і типу обслуговуючої БС (макро-, мікро-).

Підхід до вирішення задачі розміщення базових станцій заснований на послідовному виключенні базових станцій [2]. Запропонований метод оптимізує кількість і розташування базових станцій у мережі і виводить набір базових станцій.

Розрахунок відстані між користувачами і БС базується на основі зваженого розбиття Вороного, в якій враховується розподіл потужності для макро і мікро БС [3]. Призначення обслуговуючих БС до окремих користувачів відбувається шляхом розрахунку зваженої відстані між вибраним користувачем і усіма БС в мережі [4]. Алгоритм складається з шести основних кроків.

Крок 1. Вилучення БС *i* з мережі. Створення зваженого розбиття Вороного та розрахунок відстаней між усіма взаємодіючими БС після вилучення БС *i*.

Крок 2. Перевірка вимог щодо SINR для усіх користувачів в мережі.

Крок 3. Перевірка кількості користувачів, що обслуговуються кожною з БС *i* та порівняння з гранично допустимими значеннями для базових станцій макро- та мікрорівнів.

Крок 4. Перевірка вимог прийнятої потужності для кожного користувача.

Крок 5. Розміщення базової станції. Якщо існує певна кількість користувачів, що за поточних умов залишаються поза межами обслуговування (не відповідність

вимогам SINR або прийнятого рівня потужності), тоді БС *i* належить до незмінного масиву *I*.

В іншому випадку, БС *i* належить до доступного масиву *F*. Тоді, обраховується SINR у всій мережі. *F* відображає доступний набір базових станцій, що можуть бути вилучені без перевищення цільової імовірності знаходження користувача поза межами обслуговування. *I* відображає недоступний до вилучення набір базових станцій.

Крок 6. Якщо $F \neq 0$, БС з вищим значенням SINR повинна бути вилучена з мережі, а доступна множина БС зменшується на одиницю. В іншому випадку алгоритм завершує свою роботу, адже ні одна з БС не може бути вилучена з мережі без втрат. Ці кроки повторюються допоки ні одна з БС не зможе бути вилученою з мережі без спричинення втрат обслуговування.

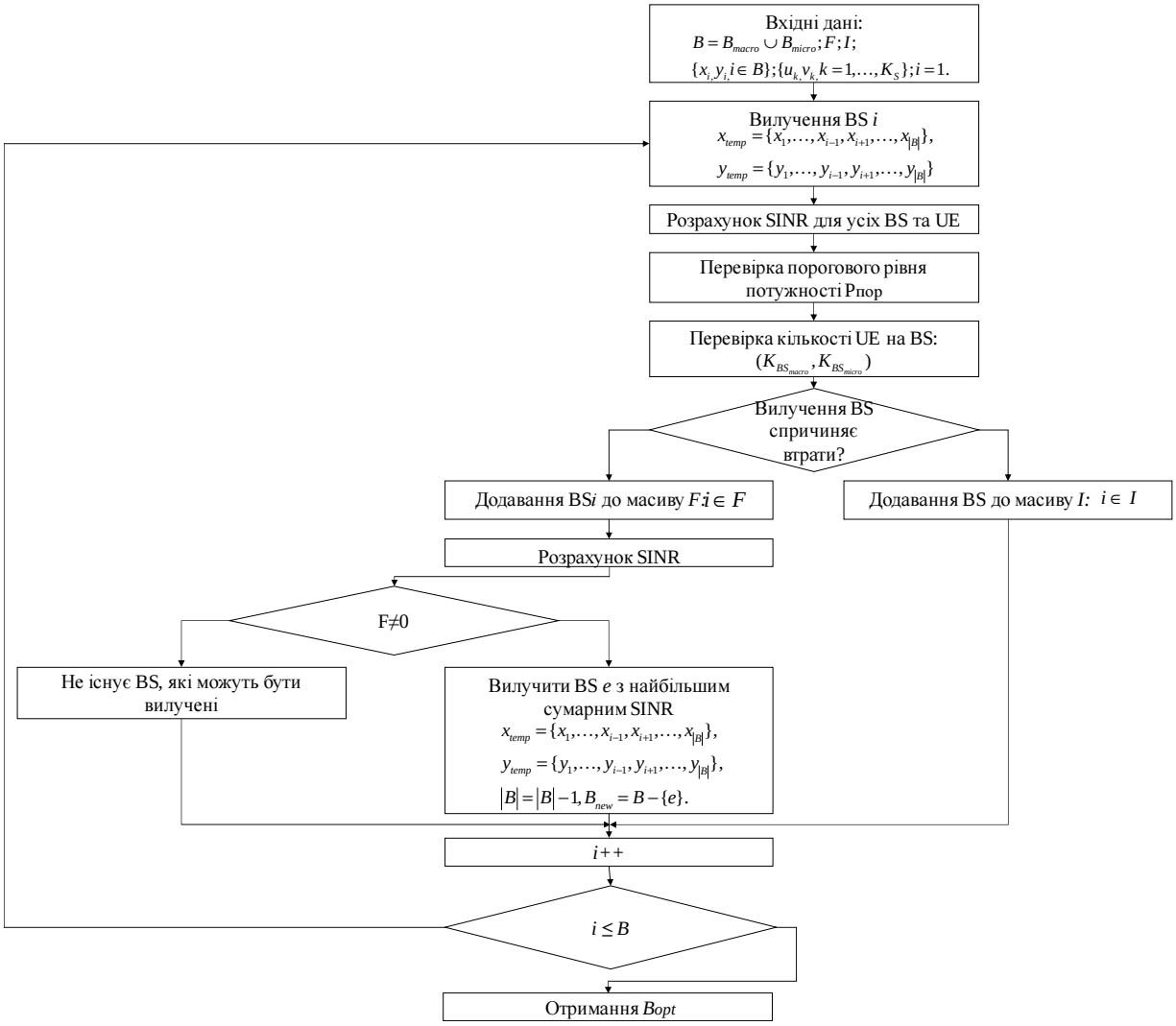


Рис.1. Блок-схема алгоритму розміщення базових станцій.

Модель мережі радіодоступу складається з множини базових станцій, що сформована з базових станцій макро- та мікро- рівнів. Макро- та мікро- БС розподіляються по території випадковим чином з різними рівнями потужності. Області концентрованого користувацького навантаження накладаються поверх рівномірного розподілу користувачів. Для наявних в даний момент активних користувачів необхідно знайти мінімально необхідну

кількість базових станцій, що забезпечує вимоги щодо радіопокриття та ємності. Приймаємо, що інтерференція залежить лише від міжкоміркової інтерференції, так як піднесучі є ортогональними в комірках в мережі, що базується на OFDMA (припускаємо ідеальну ортогональність). Для обслуговуваного UE необхідно, щоб рівень *SINR* не перевищував деякого порогового значення $SINR_{thr}$ [5]. Вираз для *SINR* може бути записаний наступним чином:

$$SINR_k = \frac{P_{k,b(k)}}{\sigma^2 + \sum_{i=1, i\neq b(k)}^{N_B} c_i P_{k,i}} \geq SINR_{thr}, \quad (1)$$

де c_i відображає, яка БС$_i$ активна в даний момент. Сума $\sum_{i=1, i\neq b(k)}^{N_B} c_i P_{k,i}$ представляє інтерференційну потужність, отриману від сусідніх БС терміналом UE$_k$.

Результати моделювання показують, що для більшості сценаріїв навантаження запропонований алгоритм дає змогу вилучити близько 40 % від загальної кількості БС при збереженні гарантованої якості обслуговування. Як правило, зони з високою щільністю користувацького навантаження покриваються великою кількістю малих комірок для забезпечення QoS.

Частка відключених користувачів (не обслуговуються ні одною БС) є 1.5%, а середня потужність прийнятого сигналу на одного користувача становить -73.2 дБм. Обидва значення знаходяться в допустимих межах.

Отримані результати характеризують основні особливості мобільних мереж наступного покоління. Малі комірки широко застосовуються для забезпечення ємності при високій концентрації користувачів, в той час як впровадження макрокомірок дає змогу покрити області з низькою щільністю користувачів.

Література

1. Huskov P.O., A Survey on Cloud Radio Access Networks Deployment Strategies / Huskov P.O., Klymash M.M // Advanced Information and Communication Technologies-2015 Lviv, October 29 – November 1, 2015), 2015, p.20-23.
2. E. Oh, K. Son, and B. Krishnamachari, “Dynamic Base Station Switching-On/Off Strategies for Green Cellular Networks,” IEEE Transactions on Wireless Communications, vol. 12, no. 5, pp. 2126–2136, May 2013.
3. J. S. Ferenc and Z. Neda, “On the size distribution of Poisson Voronoicells,” Physica A, vol. 385, no. 2, pp. 518–526, Nov. 2007.
4. Бак Р.І. Метод балансування абонентського навантаження мережі коміркового зв'язку / Бак Р.І., Чайковський І.Б., Бурачок Р.А. // Вісник Національного університету "Львівська політехніка". Радіоелектроніка та телекомунікації. – 2013. № 766. С. 110-115.
5. Яремко О.М. Метод адаптивного розподілення потужності в мобільній мережі при варіації абонентського навантаження / О.М. Яремко, Т.А. Максим'юк, Р.І. Бак // Національна академія наук України. Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова. Збірник наукових праць. – Київ, 2012. Вип. 66. – С. 137-143.

УДК 621.39

ПРОГРАММНО-АППАРАТНОЕ МОДЕЛИРОВАНИЕ ТЕЛЕКОММУНИКАЦИОННЫХ ПРОЦЕССОВ И СИСТЕМ В MATLAB С ИСПОЛЬЗОВАНИЕМ SDR И SOC ТЕХНОЛОГИЙ

Кайденко Н.Н., Кайденко В.Н.
Научно-исследовательский институт телекоммуникаций
НТУУ «КПИ», Украина, Киев
E-mail: kkk610@ukr.net

Hardware-in-the-Loop Simulation of telecommunication processes and systems in Matlab using the SDR and SoC technology

This article presents principles of Hardware-the-Loop Simulation of telecommunication processes. An example of the construction of the model, and the results of simulation of clock and phase synchronization circuits using HIL Simulation where given .

.

Программно-аппаратное моделирование (Hardware-in-the-Loop Simulation, HIL) представляет собой метод, который используется в разработке и испытании сложных технических и технологических встроенных систем реального времени. Использование программно-аппаратного моделирования позволяет проводить внутрисхемное и внутрисистемное тестирование разработанных решений и математических моделей, существенно сокращать сроки и стоимость разработки.

Процесс HIL - симуляции в общем виде состоит из трех основных этапов:

- создание математической модели реальной среды, в которой будет использоваться аппаратное устройство;
- тестирование разработанной математической модели на реальном аппаратном устройстве;
- реализация процесса в реальном устройстве с учетом результатов тестирования модели.

При HIL - симуляции возможны как варианты с математическим описанием (программной моделью) среды и внутрисхемным моделированием разрабатываемого процесса, так и с математическим описанием процесса (программной моделью) и внутрисистемным моделированием его поведения в реальной среде.

С появлением технологий программно определяемых радиосистем (Software-defined radio, SDR) и системы на кристалле (System-on-chip, SoC) возможности HIL - симуляции телекоммуникационных процессов и систем существенно расширились, чему способствовало также обеспечение поддержки такого вида симуляции программными средами моделирования, в частности Matlab. Одним из самых новых решений является использование SDR технологии Analog Devices на базеAD9361 совместно с SoC Altera или Xilinx.

Программно аппаратное моделирование телекоммуникационных

процессов и систем в Matlab базируется на использовании IIO System Object, который в свою очередь основан на спецификации системных объектов Matlab [1]. IIO System Object работает как с Matlab, так и Simulink и предназначен для обмена данными по сети Ethernet с ADI аппаратной платформой, подключенной к платформе FPGA/SoC, которая работает под управлением распределение ADI Linux.

IIO System Object построен на библиотеке libiio [2] и позволяет модели Matlab или Simulink обмениваться потоками данных с аппаратной платформой, контролировать ее установки, а также осуществлять мониторинг различных параметров. На рис. 1 представлена схема уровней, показывающая архитектуру системы.

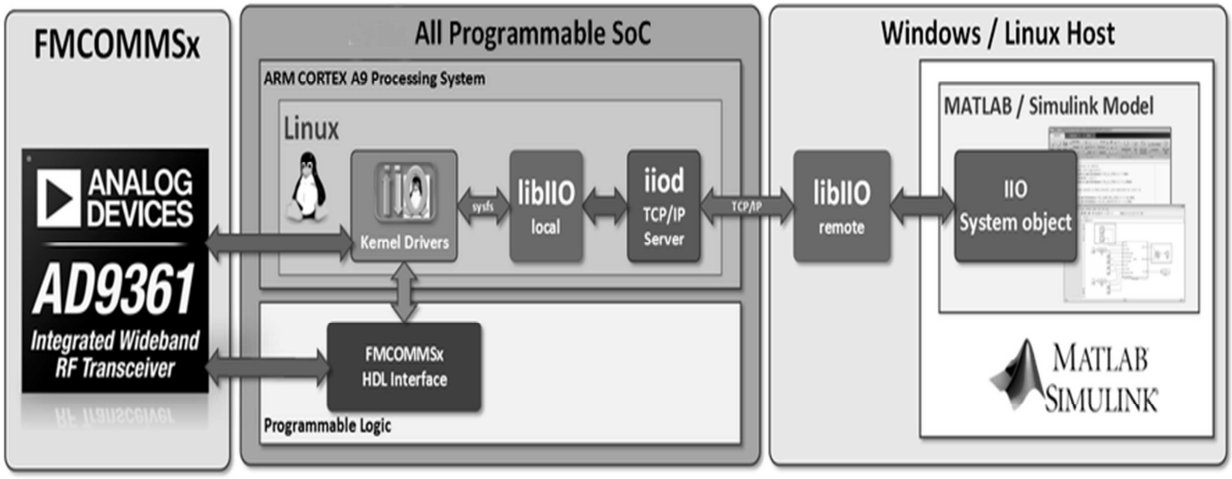


Рис.1 Схема уровней системы программно-аппаратного моделирования.

Для работы из среды Matlab с программно аппаратной платформой создается конфигурационный файл с расширением .cfg и именем, совпадающим с именем устройства, установленным в диалоговом окне конфигурации блока. Этот файл, содержит набор полей, которые определяют драйверы Linux для целевого устройства и каналы конфигурации, которые будут использоваться блоком Simulink или скрипт MATLAB. Конфигурационный файл должен содержать следующие поля:

data_in_device — имя Linux драйвера для передачи данных в устройство;
data_out_device - имя Linux драйверадля чтения данных из устройства:
ctrl_device - имя Linux драйвера для контроля и мониторинга устройства;
channel — назначение канала, последовательность параметров <имя канала, тип канала, Linux атрибуты, устройство>.

Ниже представлен пример конфигурационного файла для AD9361.

```
data_in_device = cf-ad9361-dds-core-lpc
data_out_device = cf-ad9361-lpc
ctrl_device = ad9361-phy
channel = RX_LO_FREQ,IN,out_altvoltage0_RX_LO_frequency,
.....
```

channel = TX_SAMPLING_FREQ,IN,out_voltage_sampling_frequency,
channel = TX_RF_BANDWIDTH,IN,out_voltage_rf_bandwidth.

Входные и выходные порты блока Simulink, соответствующие IIO System Object определяются посредством его свойств, а также с помощью файла конфигурации, специфичного для целевого устройства. Входные и выходные порты классифицируются как порты передачи данных и управления. Порты данных используются для приема/передачи буферов непрерывных данных из/в целевое устройство в режиме обработки кадров, в то время как порты управления используются для конфигурации и мониторинга различных параметров устройства. Число и размер портов данных настраиваются в диалоговом окне конфигурации блока, в то время как порты управления определены в конфигурационном файле.

На рис.2 показана схема модели Simulink, которая обеспечивает взаимодействие с модулем SDR на основе AD9361 посредством платформы SoC Altera CyclonV и моделирует процесс фазовой и тактовой синхронизации по алгоритмам, представленным в [3] при использовании QPSK модуляции со скруглением с индексом 0,5.

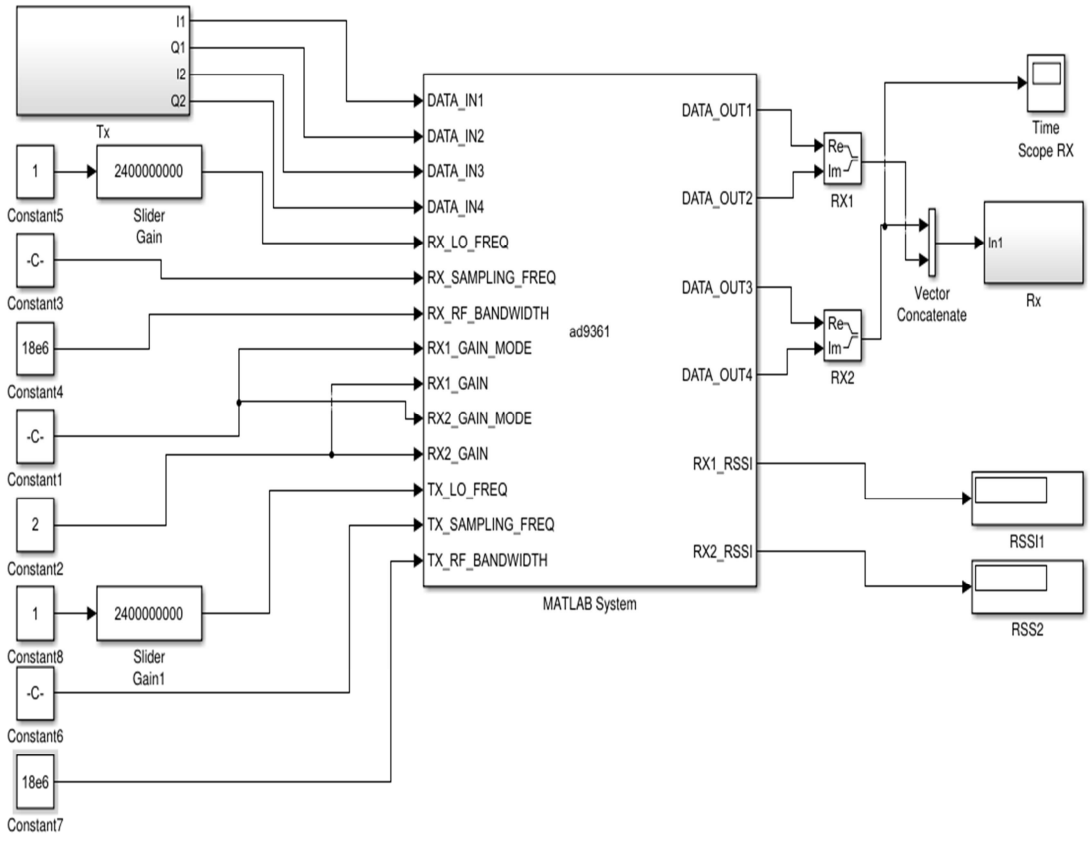


Рис.2 Схема модели Simulink, реализующая HIL симуляцию процесса фазовой и тактовой синхронизации.

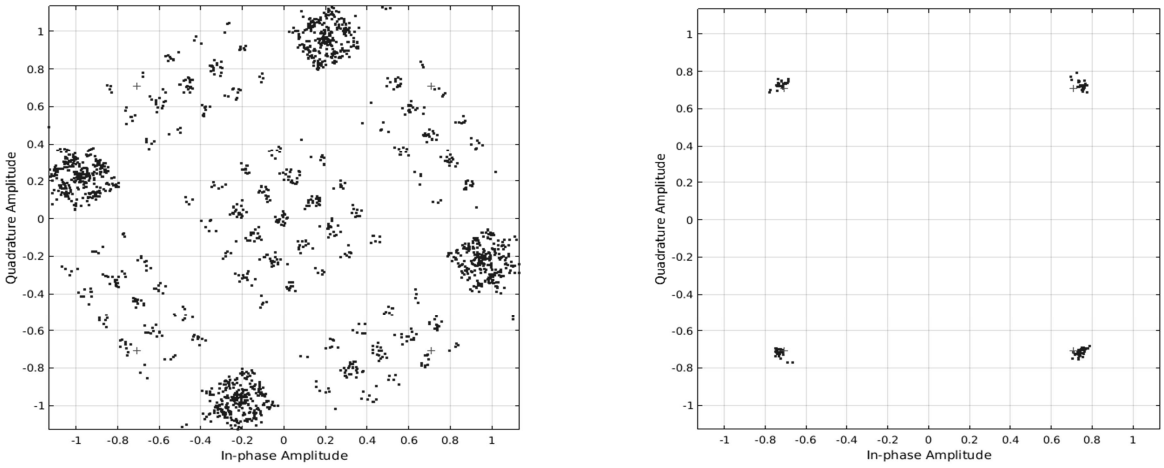
В диалоговом окне конфигурации блока настраиваются следующие параметры:

IP address - IP адрес программно аппаратной платформы;

Device name — имя устройства к которому подключается блок, причем

имя устройства и имя концигурационного файла должны быть одинаковыми;
Number of input data channels - количество входных портов данных блока;
Input data channel size — количество отсчетов входного буфера данных;
Number of output data channels - количество выходных портов данных блока;
Output data channel size - количество отсчетов входного буфера данных.

Результат симуляции показан на рис. 3: сигнальное созвездие принятых символов до фазовой и тактовой синхронизации и выборки значащего отсчета (рис а); после процесса синхронизации и выборки значащего отсчета (рис. б).



а) **б)**

Рис. 3. Результаты программно-аппаратного моделирования передачи/приема QPSK сигнала через радиоканал на основе AD9361 и работы модели схемы фазовой и тактовой синхронизации: сигнальное созвездие до синхронизации и выборки значащего отсчета (а) и после синхронизации (б).

Результаты программно аппаратного моделирования показывают, что использование этого метода позволяет более точно оценивать эффективность использования математических моделей с учетом особенностей реализации реальных телекоммуникационных устройств и систем, причем эта оценка может быть осуществлена в том числе и в реальном масштабе времени.

Литература

1. http://www.mathworks.com/help/dsp/gs/what-are-system-objects.html.
2. https://wiki.analog.com/resources/tools-software/linux-software/libiio.
3. Michael Rice, “Digital Communications: A Discrete-Time Approach”, Prentice Hall, 2008.

УДК 621.39

ОРГАНИЗАЦИЯ ВЗАИМОДЕЙСТВИЯ МЕЖДУ HPS И FPGA НА БАЗЕ SoC ТЕХНОЛОГИЙ ПРИ СОЗДАНИИ ТЕЛЕКОММУНИКАЦИОННЫХ УСТРОЙСТВ

Кайденко В.М., Кайденко М.М., Крылач О.Ф., Роскошний Д.В.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: ккк610@ukrl.net

Organization of HPS and FPGA interaction based on SoC technology for telecommunication device development

This paper gives a description of HPS+FPGA technology based on SoC, its advantages for telecommunication device development, benefits of Linux OS usage in cope with this technology, and concepts for HPS and FPGA interaction organization.

В настоящее время разработка и применение систем-на–кристалле (SoC) является одним из наиболее перспективных направлений в разработке телекоммуникационных устройств и систем. В общем случае SoC являются дальнейшим развитием технологии FPGA и представляют собой интегрированные в одном кристалле аппаратное процессорное ядро (ядра), блок программируемой логической матрицы FPGA, а также аппаратно или программно реализованные модули управления периферийными устройствами.

Внутренняя шина данных с высокой пропускной способностью свыше 10 Гбит/с, соединяющая между собой процессорное ядро и логическую матрицу FPGA, позволяет управлять периферийными модулями и в некоторых случаях ускорить выполнение алгоритмов, повышая тем самым общую производительность системы. Такой уровень интеграции не только увеличивает производительность, но и снижает мощность потребления, размеры и стоимость конечного решения [1]. Упрощенная структурная схема SoC представлена на рис 1.

Принципиальная особенность SoC - это наличие программируемых блоков. Поэтому SoC – не просто интегральная схема, а комплекс, в состав которого входят как аппаратная часть (собственно FPGA и периферийные устройства), так и программная – встраиваемое программное обеспечение. Следовательно, при проектировании SoC необходимо выполнить операции по совместной верификации и отладке взаимодействия программной и аппаратной частей [2,3].

В телекоммуникационных приложениях, в частности, в системах беспроводного широкополосного доступа, включая решения Software Defined Radio (SDR), использование технологии HPS+FPGA дает возможность ускорить разработку конечных телекоммуникационных устройств, на выходе которой можно получить мощное устройство способное обеспечить большинство необходимых вычислений в режиме реального времени

(благодаря возможности использования FPGA), которое тем не менее может легко интегрироваться в любую систему в связи с возможностью использовать такие интерфейсы как Ethernet, I2C, SPI, CAN и другие, на высоком уровне операционной системы [4].

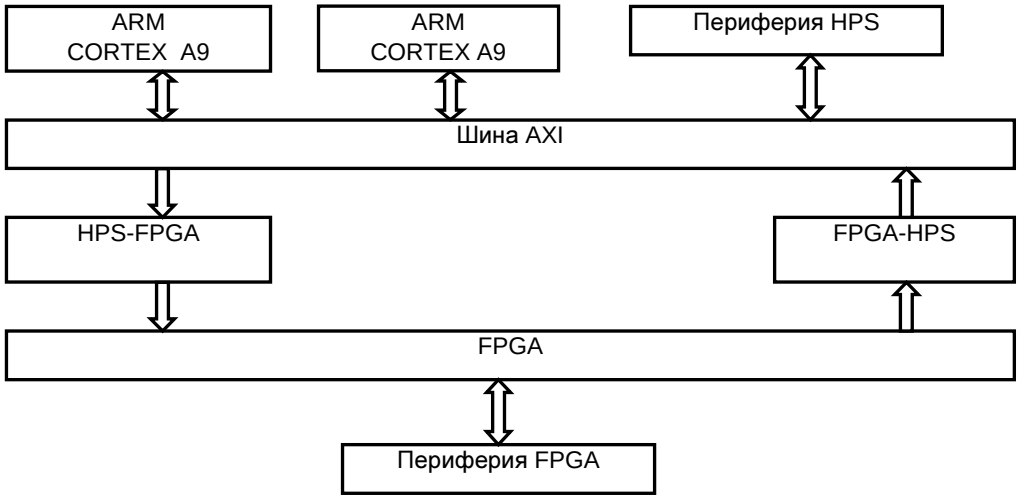


Рис. 1 Упрощенная структурная схема SoC.

Среди прочих достоинств этой технологии, применительно к SDR, особенно стоит отметить то, что она позволяет производить проектирование канала передачи данных на структурном уровне, при этом низкоуровневое проектирование будет необходимо только для реализации самых затратных с точки зрения вычислительного ресурса задач.

В разработке SoC систем существует 2 основных подхода:

- создание устройства без операционной системы (Bare Metal Application).
- использование операционной системы VxWorks/Linux

Первый подход дает возможность получения системы с максимальным уровнем производительности, но реализация его крайне сложна, так как предполагает полную разработку всех необходимых для SDR устройств, интерфейсов, и т.п. на низком уровне.

Второй подход облегчает задачу, так как на операционную систему ложится задача управления периферийными устройствами, реализации высокоуровневых протоколов обмена, таких как IP, TCP, UDP и даже протоколов доступа к устройству, например FTP, NTP, Telnet, SSH и пр.[4,5] Так же использование операционной системы позволяет создавать универсальные устройства, которые намного проще интегрировать в существующие системы, чем при использовании Bare Metal Application.

Предпочтительным является использование операционной системы Linux для SoC устройств, так как она имеет следующие преимущества [6]:

- широкая аппаратно-программная поддержка разработчика;
- огромная гибкость в приложениях готовой системы;
- простота в использовании периферийных устройств;
- наличие развитой поддержки средств разработки для встраиваемых

систем;

- на уровне ядра поддержка многоядерных процессоров и процессоров ARM.

Существует три основных подхода к организации взаимодействия HPS и FPGA в ОС Linux:

1. Использование непосредственного доступа к регистрам памяти FPGA;

2. Использование пользовательского интерфейса ввода/вывода;

3. Создание полноценного драйвера устройства Linux на функциональном уровне.

1. Простейший способ обмена данных между FPGA и процессором в обход операционной системы, который тем не менее дает возможность использовать все остальные её возможности. Взаимодействие с FPGA происходит путем прямой записи/чтения по адресам памяти, которые ей присваивает операционная система. Не позволяет использовать дополнительные возможности операционной системы и самой FPGA, такие как DMA.

2. Пользовательский интерфейс ввода/вывода операционной системы Linux позволяет создавать упрощенную версию драйверов для обмена между FPGA и центральным процессором. При таком подходе имеется возможность работать по прерываниям в операционной системе, но отсутствует возможность управления кешированием, что не дает использовать технологию прямого доступа к памяти(DMA).

3. Комплексный подход, который позволяет использовать все возможности операционной системы и FPGA при работе SoC с любой периферией, в том числе и АЦП и ЦАП в SDR. Так же позволяет один драйвер для однотипных устройств, что значительно упрощает процесс разработки готовых систем.

Использование SoC устройств совместно с SDR позволяет значительно ускорить процесс разработки беспроводных телекоммуникационных устройств и систем.

Литература

1. https://www.altera.com/content/dam/altera-www/global/en_US/pdfs/literature/br/br-industrial-brochure.pdf.
2. https://www.altera.com/content/dam/altera-www/global/en_US/pdfs/literature/wp/wp-01198-fpga-software-debug-soc.pdf.
3. https://www.altera.com/content/dam/altera-www/global/en_US/pdfs/literature/ug/ug_soc_eds.Pdf.
4. http://www.eejournal.com/files/8713/9837/5380/WP-14033__Altera_SoC_Design_Advantages_1.Pdf
5. http://www.microtoolsinc.com/Why%20Use%20Embedded%20Linux%20for%20Real%20Time%20Embedded%20Systems%20Rev%20A.pdf.
6. http://www.denx.de/en/pub/Documents/Presentations/2013-06-25-customizable-arm.pdf.

УДК 621.396.1

МЕТОД КООПЕРАТИВНОГО РОЗНЕСЕННЯ

Афанасьєва Л.О., Кравчук І.М., Кравчук С.О.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: liana.afanasyeva@gmail.com

Method of cooperative diversity

An overview of the method of cooperative diversity is presented. Gains in robustness and energy efficiency in wireless networks of the concept of cooperative diversity are considered.

Кооперативне рознесення - це метод, що базується на використанні об’єднаної множини антен для збільшення пропускної здатності каналу зв’язку для заданого набору діапазону частот. Суть методу полягає в рознесенні користувацьких терміналів шляхом декодування комбінованого ретрансляційного і прямого сигналу в бездротових багатопролітних мережах. Звичайна однопролітна система використовує методи прямої передачі даних, де приймач декодує інформацію тільки на основі прямого сигналу, а ретрансльований сигнал сприймається системою як завада. В той час, при кооперативному рознесенні додатковий сигнал сприймається в якості сигналу для співпраці, тобто інформація декодується на основі комбінації (поєднання) двох сигналів. Таким чином, кооперативне рознесення є рознесенням антен (розподіленими антенами), що належать кожному вузлу в безпроводовій мережі. Слід зауважити, що користувацька кооперація є одним із можливих варіантів кооперативного рознесення. Суть багатокористувацького рознесення полягає в тому, що в будь-який момент часу передавач вибирає «кращого» користувача серед кандидатів відповідно до якості каналу між передавачем та кожним приймачем. Отже, метод кооперативного рознесення є різновидом методу багатокористувацької техніки MIMO [1,2].

Найпростіші мережі кооперативної ретрансляції складаються з трьох вузлів, а саме джерела, адресата та вузла-ретранслятора, що підтримує прямий зв'язок між джерелом і адресатом. Якщо пряма передача повідомлення від джерела до адресата не пройшла повністю успішно, додаткова інформація (overheard information) від джерела передається через ретранслятор, щоб дістатися до адресата іншим шляхом. Так як ці два повідомлення пішли один за одним різними шляхами, в цьому випадку реалізується концепція просторового і часового рознесення.

Методи ретрансляції можуть бути додатково розділені на схеми підсилення-вперед, декодування- вперед та ущільнення-вперед.

В методі «підсилення-вперед» ретрансляційна станція підсилює прийнятий сигнал від джерела і після цього передає його до адресата.

В методі «декодування –вперед» ретранслятор «підслуховує» сигнал, що передається від джерела і в разі правильного декодування, направляє до адресата. У разі невиправних помилок у підслуханій передачі може знехтувати кооперативною передачею.

При реалізації методу «ущільнення-вперед» ретрансляційна станція

ущільнює прийнятий сигнал від вузла-джерела і направляє його без декодування до адресата. Після чого, для оптимального ущільнення може використовуватись кодування Вайнера-Зіва, яке полягає в кодуванні залежних джерел, коли потрібно ущільнення з втратами виходу першого джерела, якщо на декодері доступний без втрат вихід другого джерела.

Послідовна ретрансляційна передача використовується для посилення потужності міжміського зв'язку і розширення дальності в затінених областях. В такій топології, щоб уникнути інтерференції, сигнали поширюються від одного RN до іншого по ортогональним каналам сусідніх прольотів.

В умовах відсутності прямої видимості, довжина хвилі сигналу може бути занадто великою і установка декількох антен не представляється можливим. Тому, щоб збільшити стійкість до багатопроменевого завмиранням, що виникає при послідовній передачі, використовується паралельна передача. У цій топології сигнали поширюються по множині шляхів RN в прольотах та об'єднуються адресатом сигнали, отримані різними схемами поєднання. Така схема забезпечує підсилення по потужності та коефіцієнт підсилення від прийому рознесення одночасно.

Розглянемо безпроводову ретрансляційну систему, що складається з джерела, RN і адресата. Передбачається, що канал перебуває в напівдуплексному ортогональному ретрансляційному режимі зі схемою «підсилення-вперед». Тобто, до традиційної системи прямої передачі, ми застосовуємо функцію ретрансляційного часового розподілу, де система може передавати інформацію по двом часовим фазам.

У першій фазі, джерело передає інформацію x_s до адресата та RN. Прийнятий сигнал матиме вигляд:

$$r_{d,s} = h_{d,s} x_s + n_{d,s}$$

$$r_{r,s} = h_{r,s} x_s + n_{r,s}, (1)$$

де $h_{d,s}$ - канал від джерела до адресата, $h_{r,s}$ - канал від джерела до RN, $n_{r,s}$ - доданий до $h_{r,s}$ сигнал шуму, $n_{d,s}$ - доданий до $h_{d,s}$. сигнал шуму.

У другій фазі RN може передати отриманий сигнал до адресата в режимі прямої передачі. В разі, якщо пряма передача від джерела до адресата виявилася успішною, кооперативна передача може виявитися не тільки недоцільною, а й взагалі не потрібною.

Розглянемо чотири схеми декодування сигналу адресатом: пряма схема, некооперативна схема, кооперативна схема та адаптивна схема. В усіх схемах, крім прямої, адресатом використовується сигнал ретрансляції.

Пряма схема

В прямій схемі адресат декодує дані з сигналу від джерела у першій фазі. Так як RN не бере участі у передачі, то у другій фазі вона виключається. Декодований сигнал від джерела має вигляд:

$$r_{d,s} = h_{d,s} x_s + n_{d,s} (2)$$

Хоча схема прямого декодування проста з точки зору обробки декодування, потужність отриманого сигналу може бути дуже низькою через значну відстань між джерелом та адресатом. Тому, розглянемо некооперативну схему, що використовує сигнал ретрансляції для підвищення якості сигналу.

В некооперативній схемі адресат декодує дані на основі сингалу отриманого від RN у другій фазі, що збільшує коефіцієнт посилення по потужності сигналу. В такому випадку сигнал від RN, що отриманий від джерела має вигляд:

$$r_{d,s} = h_{d,r} r_{r,s} + n_{d,r} = h_{d,r} h_{r,s} x_s + h_{d,r} n_{r,s} + n_{d,r}, \qquad (3)$$

де $h_{d,r}$ канал від RN до джерела, $n_{r,s}$ - сигнал шуму доданий до $h_{d,r}$

Показник, що відповідає максимальній кількості одночасно діючим передачам без завад називається ступінь свободи. В некооперативній схемі ступінь свободи не збільшується сигналом ретрансляції, тому надійність декодування може бути низькою. Так як, дана схема використовує тільки ретрансльований сигнал, а прямий сигнал від джерела або відсутній або ж не враховується, то збільшення порядку рознесення не відбувається. Тому розглянемо схему, яка декодує об'єднаний сигнал від прямого і ретрансльованого вузлів.

Для кооперативного декодування, вузол призначення (адресат) об'єднує два сигнали, що отримані від джерела і ретрансляційного вузлів Весь отриманий вектор сигналу на вузол призначення може бути змодельована як:

$$r = \left[r_{d,s}\, r_{d,r}\right]^T = \left[h_{d,s} \qquad h_{d,r} h_{r,s}\right]^T x_s + \left[1 \qquad \sqrt{\left|h_{d,r}\right|^2 + 1}\right]^T n_d = \mathbf{h} x_s + \mathbf{q} n_d, \quad (4)$$

де $r_{d,s}$ та $r_{d,r}$ - сигнали, отримані вузлом призначення від джерела та RN відповідно. Як і в лінійному методі декодування, адресат поєднує елементи вектора прийнятого сигналу наступним чином: $y = \mathbf{w}^H \mathbf{r}$, (5)

де $\mathbf{w}$ - є лінійно комбінованою вагою, що може бути отримана для максимізації відношення сигнал/шум з об'єднаних сигналів, залежно (враховуючи) рівень складності розрахунку ваги.

Адаптивна схема вибирає один з трьох режимів, описаних вище, що базуються на інформації про стан каналу та інші параметри мережі.

Описано метод кооперативного рознесення, що базується на використанні об’єднаної множини антен для збільшення пропускної здатності каналу зв’язку для заданого набору діапазону частот. Досліджено схеми декодування сигналу адресатом. Показано, що реалізація схем кооперативного рознесення забезпечує підсилення по потужності та коефіцієнт підсилення від прийому рознесення одночасно.

Література

1. Building blocks of cooperative relaying in wireless systems // W. Elmenreich, N. Marchenko et al // Springer e & i. Journal–2008. –Vol. 125(10). –P. 353 - 359.
2. S. Simoens, O. Muñoz, J. Vidal, A. Del. Coso Compress-and-Forward Cooperative MIMO Relaying with Full Channel State Information // IEEE Transactions on Signal Processing.– 2010.– Vol. 58(2).– P.781 – 791.

УДК 621.396.1

ПРОПУСКНА ЗДАТНІСТЬ КАНАЛІВ З КООПЕРАТИВНОЮ РЕТРАНСЛЯЦІЄЮ

Афанасьєва Л.О.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: liana.afanasyeva@gmail.com

The channel capacity with the cooperative relaying

This paper provides an overview of transmitter channel state information. Achievable rate of a decode-and-forward relay and capacity of the time-division relaying are considered.

У системах когнітивного радіозв'язку істотно підвищити ефективність використання спектра дозволяє механізм динамічного керування спектром, відповідно до якого вторинним користувачам (не закріпленим за даним частотним діапазоном) надається можливість використовувати діапазони первинних користувачів (закріплених за даним діапазоном) на час, поки цей діапазон не використовується первинним користувачем. Просторово розподілені вузли можуть підвищити надійність моніторингу каналу за рахунок обміну інформацією та зменшити ймовірність помилкової «тривоги».

Безпроводова епізодична мережа з довільною структурою являє собою безпроводове об’єднання із самоорганізацією довільних терміналів-ретрансляторів при відсутності визначеної мережної інфраструктури. У цій мережі випадковим чином розподілені вузли утворюють тимчасову функціональну мережу і підтримувати безшовний вихід або приєднання вузлів. Такі мережі були успішно розгорнуті та мають великий потенціал для військового зв'язку, ліквідації наслідків стихійних лих, дорожньої мережі транспортних засобів для розгортання і т.д [1,2].

Бездротова сенсорна мережу може використовувати кооперативну ретрансляцію для зменшення споживання енергії в сенсорних вузлах, збільшуючи таким чином термін служби датчика мережі. Через природу безпроводового середовища, зв'язок через слабкі канали вимагає значних затрат енергії в порівнянні з відносно більш потужними каналами. Правильне впровадження кооперативної ретрансляції в процес маршрутизації може забезпечити оптимальний вибір каналів зв'язку та зберегти заряд батареї [3,4].

Слід зазначити, що за рахунок втрат безпроводового ресурсу, такого як частоти, часових та енергетичних ресурсів для фази ретрансляції, можливо збільшити коефіцієнт підсилення від прийому рознесення. Тому перед розробником систем зв'язку завжди є проблема забезпечення компромісу між коефіцієнтом рознесення і витратами ресурсів спектра при кооперативному рознесенні.

В роботі [5] проведено поглиблений аналіз пропускної здатності каналу кооперативного ретрансляційної мережі.

Припустимо, що канал від джерела до вузла ретрансляції, від джерела до вузла призначення та від вузла ретрансляції до вузла призначення є $c_{21}e^{i\varphi 21}, c_{31}e^{i\varphi 31}, c_{32}e^{i\varphi 32}$ відповідно. Вихідний вузол, вузол ретрансляції, і вузол призначення позначаються як вузол 1, вузол 2, і вузол 3, в подальшому.

Пропускна здатність каналів кооперативної ретрансляції

Використання теореми «*максимального потоку мінімального-зрізу*» дає верхню межу дуплексного ретранслювання:

$$C^{+} = \max_{f(X_1,X_2)} \min \ \{I(X_1; Y_2, Y_3|X_2), I(X_1, X_2; Y_3)\}, \quad (1)$$

де X_1 та X_2 передана інформація на вихідному вузлі і вузлі ретрансляції відповідно. Y_2 та Y_3 отримана інформація вузлом ретрансляції і вузлом призначення відповідно. Відмітимо, що теорема максимального потоку мінімального-зрізу полягає у тому що максимальний обсяг потоку дорівнює пропускній здатності мінімального розрізу, тобто є вузьким місцем. Пропускна здатність широкомовного каналу з X_1 до Y_2 та Y_3 з заданою X_2 розраховується як:

$$\max_{f(X_1,X_2)} I(X_1; Y_2, Y_3|X_2) = \frac{1}{2}\log(1 + (1-\beta)(c_{21}^2 + c_{31}^2)P_1 \quad (2)$$

в той час як пропускна здатність каналу множинного доступу від X_1 та X_2 до Y_3 буде

$$\max_{f(X_1,X_2)} I(X_2, X_2; Y_3) = \frac{1}{2}\log\left(1 + c_{31}^2 P_1 + c_{32}^2 P_2 + 2\sqrt{\beta c_{31}^2 c_{32}^2 P_1 P_2}\right) \quad (3)$$

де β - це кількість кореляції між X_1та X_2. Слід звернути увагу, що X_2 копіює якусь частину X_1 для можливості кооперативної ретрансляції.

Використовуючи можливості кооперативної ретрансляції на вузлі ретрансляції підвищується продуктивність прийому в вузлі призначення. Таким чином, верхню межу переписано у вигляді:

$$C^{+} = \max_{0\le\beta\le 1} \min \ \left\{\frac{1}{2}\log(1 + (1-\beta)(c_{21}^2 + c_{31}^2)P_1), \frac{1}{2}\log\left(1 + c_{31}^2 P_1 + c_{32}^2 P_2 + 2\sqrt{\beta c_{31}^2 c_{32}^2 P_1 P_2}\right)\right\} \quad (4)$$

Досяжна швидкість в схемі «декодування-вперед»

За рахунок декодування на RN, значення досяжної швидкості розраховується наступним чином:

$$R_1 = \max_{f(X_1,X_2)} \min \ \{I(X_1; Y_2, Y_3|X_2), I(X_1, X_2; Y_3)\} \quad (5)$$

де широкомовний канал зводиться до каналу точка-точка через декодування в вузлі реле, тобто $I(X_1; Y_2, Y_3|X_2)$ зводиться до $I(X_1; Y_2|X_2)$. Пропускна здатність відновленого широкомовного каналу буде:

$$\max_{f(X_1,X_2)} I(X_1; Y_2, |X_2) = \frac{1}{2}\log(1 + (1-\beta)c_{21}^2 P_1) \quad (6)$$

Таким чином, досяжна швидкість переписується у вигляді:

$$R_1 = \max_{0\le\beta\le1} \min \left\{\frac{1}{2}\log(1 + (1-\beta)c_{21}^2 P_1), \frac{1}{2}\log\left(1 + c_{31}^2 P_1 + c_{32}^2 P_2 + 2\sqrt{\beta c_{31}^2 c_{32}^2 P_1 P_2}\right)\right\} \quad (7)$$

Ретрансляція з часовим розділенням каналів

Верхня межа пропускної здатності каналу ретрансляції з часовим розділенням має вигляд:

$$C^+ = \max_{0\le\beta\le1} \min \{C_1^+(\beta), C_2^+(\beta)\} \quad (8)$$

з

$$C_1^+(\beta) = \frac{\alpha}{2}\log\left(1 + \left(c_{31}^2 + c_{21}^2\right){P_1}^{(1)}\right) + \frac{1-\alpha}{2}\log\left(1 + (1-\beta)c_{31}^2 {P_2}^{(1)}\right) \quad (9)$$

$$C_2^+(\beta) = \frac{\alpha}{2}\log\left(1 + c_{31}^2 {P_1}^{(1)}\right) + + \frac{1-\alpha}{2}\log\left(1 + c_{31}^2 {P_1}^{(2)} + c_{32}^2 P_2 + 2\sqrt{\beta C_{31}^2 {P_1}^{(2)} C_{32}^2 P_2}\right) \quad (10)$$

Досліджено пропускну здатність каналу кооперативного рознесення. Показано, що при кооперативному рознесенні додатковий сигнал сприймається в якості сигналу для співпраці, тобто інформація декодується на основі комбінації (поєднання) двох сигналів. Реалізація схем кооперативного рознесення забезпечує підсилення по потужності та коефіцієнт підсилення від прийому рознесення одночасно.

Література

1. Building blocks of cooperative relaying in wireless systems // W. Elmenreich, N. Marchenko et al // Springer e & i. Journal–2008. –Vol. 125(10). –P. 353 - 359.
2. S. Simoens, O. Muñoz, J. Vidal, A. Del. Coso Compress-and-Forward Cooperative MIMO Relaying with Full Channel State Information // IEEE Transactions on Signal Processing.– 2010.– Vol. 58(2).– P.781 – 791.
3. Ilchenko M.Yu., Kravchuk S.O. Telecommunication broadband access systems. – Kiyiv: Naukova Dumka, 2009. – 312 p.
4. Кравчук С.О. Модель імовірності помилки в багатоантенній кооперативній ретрансляційній системі // Зб. наукових праць Військового інституту телекомунікацій та інформатизації Національного технічного університету України "Київський політехнічний інститут". – К.: ВІТІ НТУУ "КПІ", 2009. – Випуск № 2. – С. 47–62.
5. A. Host-Madsen, J. Zhang Capacity bounds and power allocation for wireless relay channels // IEEE Transactions on Information Theory.–2005.– Vol. 51(6).– P.2020 – 2040.

УДК 621.396.1

МОДЕЛЬ БАГАТОСТІЛЬНИКОВОЇ МЕРЕЖІ З MIMO - КООПЕРАЦІЄЮ

Афанасьєва Л.О., Кравчук І.М., Кравчук С.О.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: liana.afanasyeva@gmail.com

Model of Multi-Cell MIMO Cooperative Network

An overview of the different possible levels of cooperation are presented. The models for the network and signals and the way that information is exchanged between the cells are considered.

Схеми звичайного рознесення та ретрансляції значно покращують продуктивність та надійність на канальному рівні, але мало ефективні щодо якості обслуговування користувачів, що знаходяться в областях з високою міжсотовою інтерференцією (області меж сот в стільникових мережах). Виходячи з вище сказаного, боротися з інтерференцією слід за допомогою спеціальних підходів, таких як "віртуальна" або "мережева" MIMO таким чином, щоб максимізувати кількість суміщених каналів зв'язку, які можуть співіснувати з прийнятною якістю обслуговування. В режимі з високим відношенням сигнал/шум цей показник якості відповідає максимальній кількості одночасно діючих передач без завад та називається ступінь свободи (degree of freedom) або коефіцієнтом підсилення мультиплексування мережі [1,2].

Розглянемо багатостільникову мережу, що включає *M* базових станцій BS, що взаємодіють та працюють на однаковій несучій частоті. Кожний стільник обслуговує *K* користувачів. Кожна BS оснащена *J* антенами. Користувачі мають одноантенні термінали. Огляд в основному представлено с точки зору інтерференції на стороні BS. Багатоантенні термінали дозволяють забезпечити просторове мультиплексування безлічі потоків даних для кожного користувача. Також, їх використання є ефективним щодо можливості придушення багатостільникової інтерференції на стороні користувача, особливо в контексті координації інтерференції.

В висхідній лінії зв'язку, прийнятий сигнал на m -й базовій станції, $m \in [1, M]$ можна записати у вигляді:

$$y_m = \sum_{l=1}^{M} \sum_{k=1}^{K} h_{m,l,k}\, x_{l,k} + z_m \qquad (1)$$

де $x_{l,k}$ - символ, що передається до k –ї MS в l- му стільнику, $h_{m,l,k}$ - позначає J елемент вектора каналу від k –го мобільного терміналу MT в l –му стільнику до m –ї BS, **z** - є вектор шуму, що містить адитивний шум і будь-яку міжсотову інтерференцію не враховується виключно M взаємодіючими стільниками, наприклад, якщо мережа включає більше M BS.

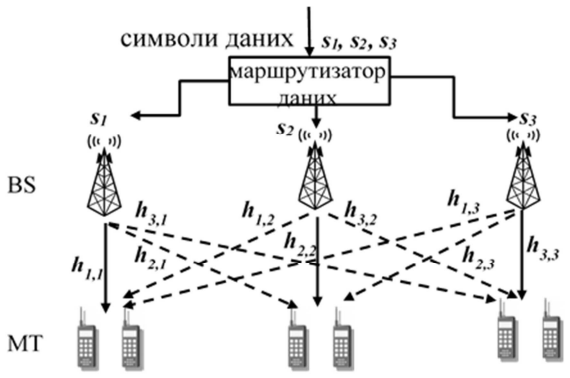
Модель для низхідної лінії зв'язку може бути легко отримана з наведеної вище. Сигнал, прийнятий на k -го MS в m –му стільнику записується у вигляді:

$$y_{m,k} = \sum_{l=1}^{M} h_{l,m,k} x_l + z_m \quad (2)$$

де x_l вектор переданого сигналу з J елементів, переданих з l-й BS, що містить, можливо, попередньо кодовані інформаційні символи для декількох користувачів. Слід зазначити, що вектор каналу низхідної лінії зв'язку від l-й BS до k –го MS в m - му стільнику позначається у комплексній кон'югованій формі відповідного каналу висхідної лінії $\mathbf{h}_{l,m,k}$.

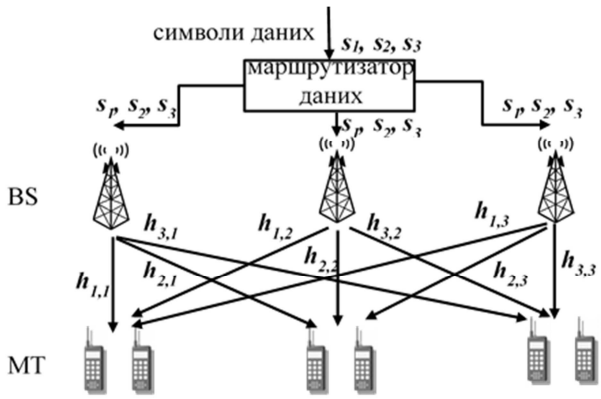
Координація рівня інтерференції

Продуктивність сучасних стільникових мереж можна поліпшити за умови забезпечення між BS обміну інформацією про стан прямого та зворотного каналів, отриману від користувацьких терміналів по каналах зворотного зв'язку. Наявність інформації про стан каналу дозволяє базовим станціям координувати сигнальну стратегію (розподіл потужності, напрями формування діаграми спрямованості), а також часове та частотне розподілення між користувачами. Такий базовий рівень координації вимагає відносно невеликої кількості транзитних зв'язків і може бути досить ефективним, якщо достатня кількість користувачів співіснувати в системі (багатокористувацького рознесення) [3]. Не має необхідності в обміні даними передачі та синхронізації рівня сигналу між базовими станціями. Такі схеми називаються *схемами з координацією рівня інтерференції.* У цьому випадку сигнал низхідної лінії зв'язку в l-й базі, $\mathbf{x}_l$ - є комбінацією символів, призначених для кожного *К-го* користувача.



а

Рис. 1 Схема координації рівня інтерференції для низхідної лінії зв'язку, де s_1, s_2, s_3 – -«пілотні» сигнали, h_{ij} - коефіцієнти передачі між i приймальними антенами j та передавальними.



б

Рис. 2 Багатостільникова MIMO для низхідної лінії зв'язку, де s1, s2, s3 – поток даних кількох користувачів.

Слід зауважити, що BS отримують та обмінюються інформацією тільки про стан каналу відносно всіх прямих та зворотних ліній зв’язку, а не символи даних (рис. 1). Наявність інформації про стан каналу дозволяє реалізувати стратегію передачі даних по різних стільниках для спільної адаптації до стану каналу. Стратегії передачі можуть включати в себе планування, управління потужністю, формування діаграми спрямованості, а також сучасні методи кодування, спеціально розроблені для послаблення

інтерференції.

MIMO - кооперація

Коли базові станції(кожна з яких оснащена *J*-антенами) пов'язані лініями зв’язку високої ємності без затримок, вони можуть поширювати інформацію не тільки про стан каналу, а також повними даними про своїх відповідних користувачів (рис. 2). Таким чином, комбіноване застосування декількох антен BS, що відносяться до різних стільників для відправки або отримання потоків даних кількох користувачів імітує модель великого MIMO масиву з *MJ* антенами і називається *MIMO - кооперацією* .

В даній схемі зникає концепція індивідуально обслуговуючої бази для одного терміналу, оскільки мережа в цілому, або принаймні група стільників, обслуговують користувацький термінал. Таким чином досягається ефективніша форма кооперації (співпраці). В загальному випадку MIMO кооперація перетворює багатостільникову мережу в багатокористувацький MIMO (MU-MIMO) канал, для якого всі канали розповсюдження (у тому числі й зворотні) експлуатуються для передачі корисних даних шляхом попереднього кодування/декодування. Таким чином, сигнал низхідної лінії зв'язку $\mathbf{x}_l$ є комбінацією символів, призначених для всіх *MK* користувачів. Для порівняння, схеми з координацією рівня інтерференції спрямовані на зменшення створених завад, а не використовують їх. Наприклад, якщо базові станції обладнані безліччю антен, формування діаграми спрямованості може бути використане в кожному стільнику. У цьому випадку промені зазвичай намагаються знайти компроміс між усуненням міжсотової інтерференції та збільшенням до максимуму отриманої енергії від/для користувача всередині стільника. В ідеальному випадку вибір таких пучків координується на декількох стільниках.

Хоча основні теоретичні концепції MIMO добре зрозумілі, все ще існує необхідність в подальших дослідженнях систем з кооперацією. На відміну від стандартних MIMO систем, де витрати багатоантенної обробки пов'язані з додатковим апаратним і програмним забезпеченням в окремих пристроях, кооперативні методи MIMO не потребують обов'язкових додаткових антен. MIMO кооперація дає додаткові переваги в порівнянні з простішими схемами координації формування діаграми спрямованості, але це вимагає поширення даних користувача між декількома BS і більш складну процедуру попереднього кодування і декодування.

Література

1. Multi-Cell MIMO Cooperative Networks: A New Look at Interference//D. Gesbert ; S. Hanly et al // IEEE Journal on Selected Areas in Communications. –2010. –Vol. 28, №. 9. –P. 1380 - 1408.
2. Fehske A., Viering I, Voigt J, Sartori C., Redana S.,Fettweis G. Small Cell Self-Organizing Wireless Networks // Proceedings of the IEEE.–2014.– Vol. 102, № 3.– P.334 – 350.
3. Гудименко І.А., Кравчук С.О. Технологія кооперативного MIMO в мультимедійних безпроводових сенсорних мережах // Зб. тез 4-ї міжнародної науково-технічної конф. «Проблеми телекомунікацій», 20–23 квітня 2010 р., Київ. – Київ: ВД «ЕКМО», 2010. – С. 101.

УДК 621.396.1

ПРОЦЕДУРИ ВЕРТИКАЛЬНОЇ ПЕРЕДАЧІ ОБСЛУГОВУВАННЯ ДЛЯ БЕЗПРОВОДОВИХ МЕРЕЖ 4-ГО ПОКОЛІННЯ

Довгань Б.М, Кравчук С.О.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: Sniperjd@mail.ua

Vertical handover decision processes for fourth generation wireless networks

Different type of decisions processes for optimization fourth generation wireless networks was considered.

На сьогоднішній день безпроводові технологій зв’язку стали невід'ємною частиною повсякденного життя і продовжують інтегруватись в нові сфери людської діяльності. Зростаючий споживчий попит на доступ до послуг телекомунікацій в будь-який час, в будь-якому місці, прискорює технічний розвиток в напрямку інтеграції різних технологій безпроводового доступу. Така інтеграція поєднує поодинокі мережі доступу в єдину систему, яку називають мережею четвертого покоління (4G) безпроводових систем. Такі системи 4G забезпечують високі швидкості передачі даних, пропонують широкий спектр послуг і застосувань, які раніше було складно використовувати через обмеження пропускної здатності, і дозволяють глобальний роумінг серед різноманітних мобільних мереж доступу [1, 2].

У безпроводовому середовищі систем 4G, мобільний користувач може продовжувати використання мобільного пристрою під час переміщення від однієї точки доступу до іншої. Такий процес називається передачею обслуговування (ПОб), за допомогою якого мобільний термінал зберігає своє з'єднання активним, під час зміни зони покриття однієї точки доступу до іншої [3].

Алгоритми вертикальної ПОб допомагають мобільним терміналам вибрати найкращу мережу для підключення серед всіх можливих варіантів. На відміну від алгоритмів горизонтального рішення про передачу обслуговування, які в основному розглядають потужність сигналу (RSS), в якості критеріїв прийняття рішення для алгоритмів вертикальної ПОб є такі критерії, як вартість послуг, споживаної потужності і швидкості мобільного терміналу [4].

У мережах 4G гетерогенного характеру користувачі можуть мати часті ПОб. Тому, щоб забезпечити нерозривний роумінг та ефективне використання ресурсів мережі, широко використовуються інтелектуальні алгоритми вертикальної передачі обслуговування. В даній роботі розглядається дана проблема і пропонуються методи оптимізації схеми передачі обслуговування, що мінімізує помилки в процесі передачі, помилково ініційовані процедури ПОб та переривання зв’язку. Крім того,

методи також забезпечують механізми мобільних застосувань для контролю компромісу між доцільністю використання мережі та кількістю процедур передачі обслуговування чи переривань з'єднань [3].

Три етапи беруть участь в процесі вертикальної передачі обслуговування:

- виявлення мережі;
- рішення про передачу обслуговування;
- передача обслуговування [4].

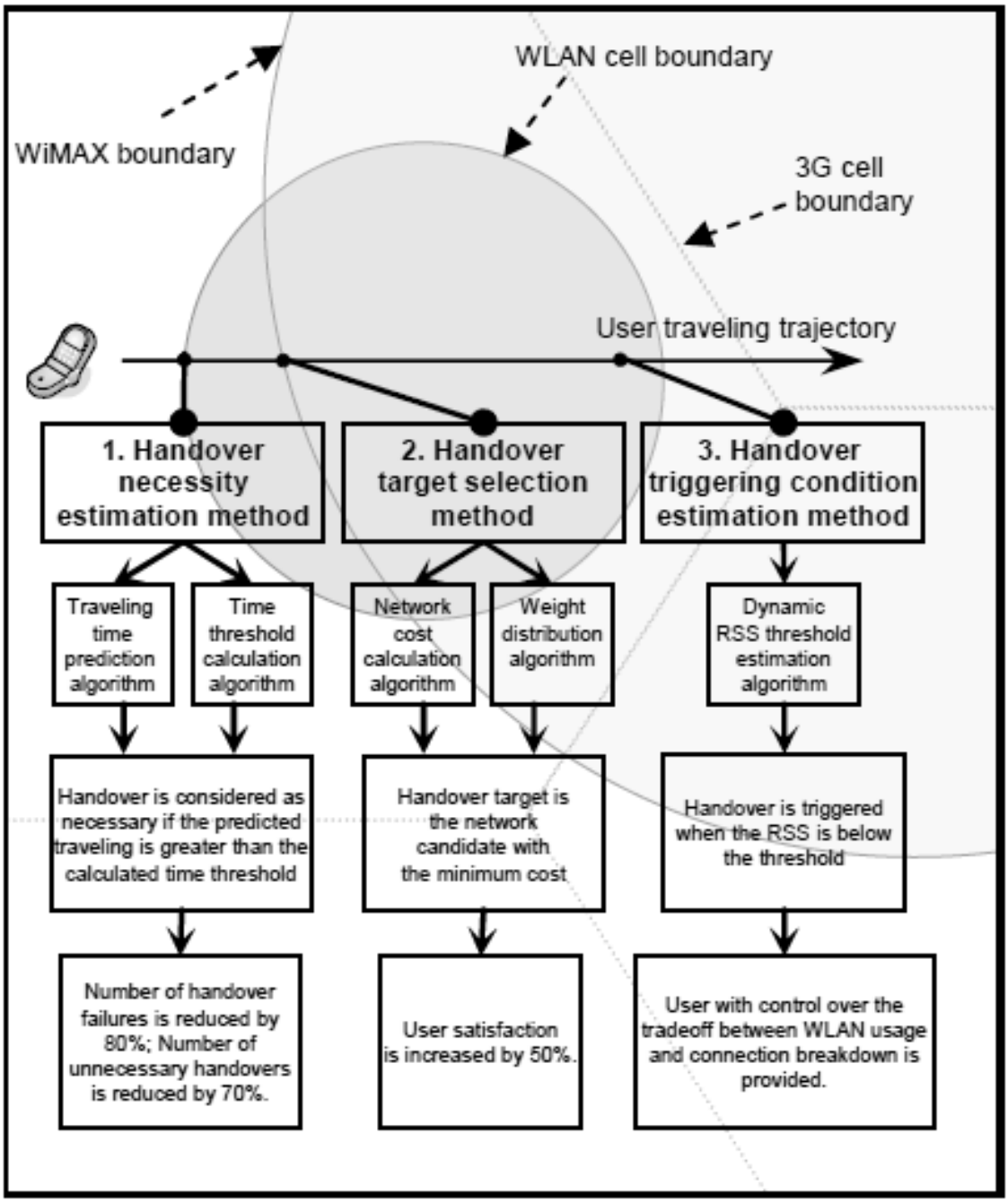


Рис. 1. Три основні компоненти проекту та їх внесок.

Метою цієї структури є забезпечення оптимізованого рішення про передачу обслуговування, яка:

- зводить до мінімуму непотрібні і невдалі ПОб з використанням блоку оцінки необхідності передачі обслуговування;

-максимізує задоволення користувачів, використовуючи направлений блок вибору передачі обслуговування. Метод, що передбачає обчислення коефіцієнта витрат та значень різних мережних параметрів, які генеруються на основі призначених для користувача переваг і рівня потужності мобільного терміналу. Алгоритм розрахунку фактора витрат оцінює витрати на передачу, аналізуючи мережу кандидата за допомогою функції, що проводить оцінку мережевих параметрів в якості вхідних даних і генерує фактори вартості для всіх мереж. Мережа з найменшим коефіцієнтом витрат вибирається в якості цільової для передачі обслуговування. Цей метод може максимізувати задоволеності користувачів до 50%, в порівнянні з методами, які послідовно обирають мережу доступу.

- зберігає ймовірність розриву з'єднання в межах бажаних рівнів;

-надає користувачеві контроль над компромісом між ймовірністю розриву підключення і використання WLAN.

Ефективна вертикальна передача обслуговування залишається вирішальним фактором в реалізації мобільних технологій 4G. В даній роботі було розглянуто основні проблеми, які мають місце при передачі обслуговування, також проаналізовано існуючі методи оптимізації, що покращують ефективність гетерогенних безпроводових мереж.

Запропонований метод розроблений для мінімізації збоїв передачі обслуговування і уникнення непотрібних передач обслуговування від мереж стільникового зв'язку до WLAN, оцінюючи необхідність передачі обслуговування. Оцінка включає два етапи: прогнозування часу подорожі і розрахунку порогового часу.

Граничні значення часу розраховуються на основі різних параметрів мережі, таких як ймовірність відмови передачі обслуговування або ймовірності непотрібної передачі обслуговування, радіусу покриття WLAN і затримки передачі обслуговування. Цей спосіб може зменшити число збоїв передачі обслуговування, і непотрібних передач обслуговування до 80% і 70%, в порівнянні зі звичайними RSS на основі гістерезису.

Література

1. Evolution and emerging issues in mobile wireless networks / S. Dekleva, J. P. Shim, U. Varshney, and G. Knoerzer. // Communications of the ACM. – 2007. - **50**(6). – P. 38–43.
2. Ільченко М.Ю., Кравчук С.О. Телекомунікаційні системи широкосмугового радіодоступу. – К.: Наукова думка, 2009. – 312 с.
3. Nasser N., Hasswa A., Hassanein H. Handoffs in fourth generation heterogeneous networks // IEEE Communications Magazine. – 2006. – 44. – P. 96–103.
4. Wang, P., Akyildiz, I.F. On the Stability of Dynamic Spectrum Access Networks in the Presence of Heavy Tails // IEEE Transactions on Wireless Communications. – 2015. -vol. 14, no. 2. – P. 870-881.

УДК 621. 396.1

ЗМЕНШЕННЯ ВПЛИВУ СПІВКАНАЛЬНИХ ЗАВАД В БЕЗПРОВОДОВИХ МЕРЕЖАХ З РЕТРАНСЛЯЦІЄЮ

Кисельов В. О., Кравчук С. О.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: slavko_kiselev@ukr.net

Minimizing Co-Channel Interference in Wireless Relay Networks

The use of multi-hop relaying in cellular networks is considered a key technique for increasing data transmission rates and maximizing coverage in fourth generation (4G) wireless systems. This paper presents an algorithm whose purpose is to find the best relay or set of relays

При рішенні завдань, пов'язаних зі збільшенням площі покриття і місткості безпровідної стільникової мережі зв'язку, викликає великий інтерес концепція багатопролітної ретрансляції [1-3]. Так введення фіксованої mesh топології, що відноситься до ретрансляційних мереж, стало одним з поліпшень стандарту IEEE 802.16-2004 [4].

У ретрансляційній мережі є певна кількість ретрансляційних станцій (РС), які братимуть участь в доставці даних від точки доступу мережі (ТД) до мобільного терміналу (МТ). Кожна РС повністю забезпечуватиме покриття невеликого регіону (мікростільники) з діаметром 200..500 м (в порівнянні з діаметром стільника в 2..5 км в традиційній стільниковій системі) [1] . Це дає дві переваги: шлях поширення радіохвилі скорочується так, що втрати на поширення знижуються, а шлях сигналу може бути маршрутизований так, щоб обійти навколо перешкод для зниження ефекту затінювання. За допомогою цих досліджень було показано, що, незважаючи на потребу в додатковому радіоспектрі для ретрансляційних прольотів, існує відчутне збільшення повної місткості мережі.

Дана робота розглядає прямий канал передачі (downlink) фіксованих РС (ФРС). Оскільки існує велика кількість ФРС в мережі, то вони мають бути недорогими і простими для того, щоб така мережа була досить економічною. Інтелект мережі зосереджений в ТД, яка управляє трафіком і численними ФРС в межах досить великого діаметру (порівнянного з діаметром макростільників в традиційній стільниковій мережі). ТД відповідальна за вибір кращого ФРС чи ряду ФРС для передачі інформації на

МТ, а також вибору (маршрутизації) кращого шляху ретрансляції до МТ. Більшість досліджень розглядають вибір тільки окремою ФРС для передачі інформації МТ. Ця робота торкається вибору кращої одиничної або групи ФСР, розрахунку потужності передачі для мінімізації соканальної інтерференції між зонами покриття ФРС. Переваги такого підходу наступні: додатковий ступінь свободи при виборі ФРС, можливість використання рознесення або розподіленої багатоантенної техніки MIMO (Multiple Input - Multiple Output), і додаткове зниження затінювання за допомогою можливості вибору обхідного шляху перешкоди.

Розташування кожного МТ знаходиться під контролем ТД, також як і передача інформації від ФРС до МТ. Алгоритм, пропонований в справжній роботі, дозволяє розрахувати оптимальну потужність передачі в прямому каналі від ФРС, враховуючи як інформацію про втрати на поширення до цільового МТ, так і відносне положення потенційного приймача перешкод від ФРС.

На мал. 1 показана узагальнена системна модель з численними ФРС під управлінням однієї ТД, які можуть перешкоджати на своє задіювання для передачі інформації на цільовий МТ. Є однозначний транспортний маршрут (п. 3 на мал. 1) передачі даних через вибрані ФРС і існують також можливі шляхи доступу від кінцевого в транспортному маршруті ФРС до цільового МТ (тільки один такий шлях показаний на мал. 1). Маршрутизація від ТД до вибраних ФРС представляється як роздільне завдання.

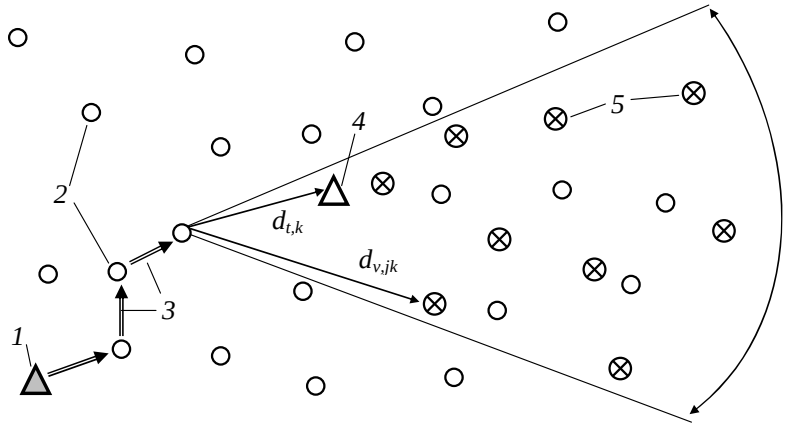


Рис. 1. Загальна системна модель:

1 - ТД; 2 - ФРС; 3 - однозначний транспортний маршрут; 4 - цільовий МТ; 5 - МТ, які перебувають під впливом перешкод

Приведений коефіцієнт передачі (КП) від ФРС до цільового МТ може бути записаний у виді:

$$\gamma_{t,k} = \xi_{t,k} d_{t,k}^{-\beta}, \quad (1)$$

де k = 1, 2, … b; β - коефіцієнт втрат на поширення; $\xi_{t,k}$ - випадкова величина, що моделює багатопутні завмирання; $d_{t,k}$ - відстань від цільового МТ до ФРС$_k$; b - кількість ФРС, що розглядаються як потенційні кандидати для встановлення через них шляхи передачі даних.

Загальна приведена потужність, що приймається на МТ, буде рівна

$$P_r = \sum_{k=1}^{b} \gamma_{tk} P_k, \quad (2)$$

де P_k - потужність передачі від ФРС$_k$.

На приймачі повинна підтримуватися мінімальна потужність $P_{\min}$, при якій коефіцієнт помилок не перевищує заданого значення

$$P_{\min} = \sum_{k=1}^{b} \gamma_{t,k} P_k. \quad (3)$$

Було показано значне поліпшення зменшення вірогідності відмови, яке було досягнуте в "ретрансляційній мережі багатострибковим шляхом виділення потужностей даунлінка, що передаються, розглядаючи канали цільових мобільних служб зв'язку і потенційних " жертв" інтерференції.

Представлений нелінійний алгоритм, що дозволяє визначити передаванні потужності від безлічі передавальних базових станцій, що полегшують використання багатоскладних антенних технологій.

Література

1. R. Pabst et al., “Relay-based deployment concepts for wireless and mobile broadband radio,” IEEE Commun. Mag., vol. 42, pp. 80–89, Sept. 2004.
2. J. Jun and M. Sichitiu, “The nominal capacity of wireless mesh networks,” IEEE Commun. Mag., vol. 41, pp. 8–14, Oct. 2003.
3. N. Esseling, B. Walke, and R. Pabst, Fixed Relays For Next Generation Wireless Systems. New York, USA: Springer Science& Business Media, Inc., 2005, ch. 5, pp. 71–91.
4. Air Interface for Fixed Broadband Wireless Access Systems, IEEE Std. 802.16-2004.

УДК 621.396.1

ДОСЛІДЖЕННЯ ЕНЕРГОЕФЕКТИВНОСТІ ДЛЯ МІКРОСОТОВИХ БАЗОВИХ СТАНЦІЙ

Мєлєхова М.О., Кравчук С.О.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: maria.melekhova@gmail.com

Research efficiency for microcellular base stations

Describing microcell base stations ways to reduct in power consumption. Comparing the energy efficiency WiMAX, HSPA, LTE of microcell base stations. The most energy-efficient technology is mobile WiMAX for bit rates higher than 3.8 Mbps. The bit rates between 2.8 Mbps and 3.8 Mbps LTE is the most energy-efficient technology. Bit rates lower the 2.8 Mbps are barely compatibled by HSPA.

Інформаційно-комунікаційні технології відповідають за 4% світового споживання первинної енергії. Цей відсоток у найближчі 10 років може зрости у двічі. 9% від загальної цифри – споживання мережами радіодоступу, в яких лише 10% енергії споживається терміналами, а 90% - базовими станціями. Отож питання оптимізації витрат енергії для базових станцій буде дуже актуальним найближчі декілька років[1].

Мережі мають ієрархічну структуру. Можуть бути використані макрос тільникові, мікростільникові, пікостільникові мережі. Максимальний діапазон охоплення мають макростільникові мережі, мікростільникові мають менший радіус покриття і використовуються в густозаселених міських районах. Пікостільникові мережі набагато менші мікростільникових і використовуються зазвичай для внутрішнього освітлення у великих будівлях. Щоб визначити споживання потужності всієї безпровідної мережі, споживана потужність базових станцій повинна бути змодельована. Безпровідні технології, які будуть досліджені у статті: WiMAX, HSPA, LTE.

Споживана потужність охопленої ділянки визначається за формулою:

$$PC_{area} = \frac{P_{el/micro}}{\pi \cdot R^2} \qquad (1)$$

Чим нижче PC_{area}, тим більш енергоефективною є технологія.

Базова станція складається обладнання, необхідного для зв’язку з мобільними станціями, так і для транзитної мережі. Мікростільникова базова станція показана на рис.1 і складається з приймач, цифрової обробки сигналів, підсилювач потужності, перетворювач змінного струму в постійний або випрямляч і кондиціонер повітря. На відміну від макростільникової базової станції, міктостільникова підтримує тільки один сектор, і кожен компонент використовується один раз. Споживана потужність $P_{el/amp}$ підсилювача потужності залежить від необхідної вхідної потужності P_{Tx} антени і визначається:

$$P_{el/amp} = \frac{P_{Tx}}{\eta} \qquad (2)$$

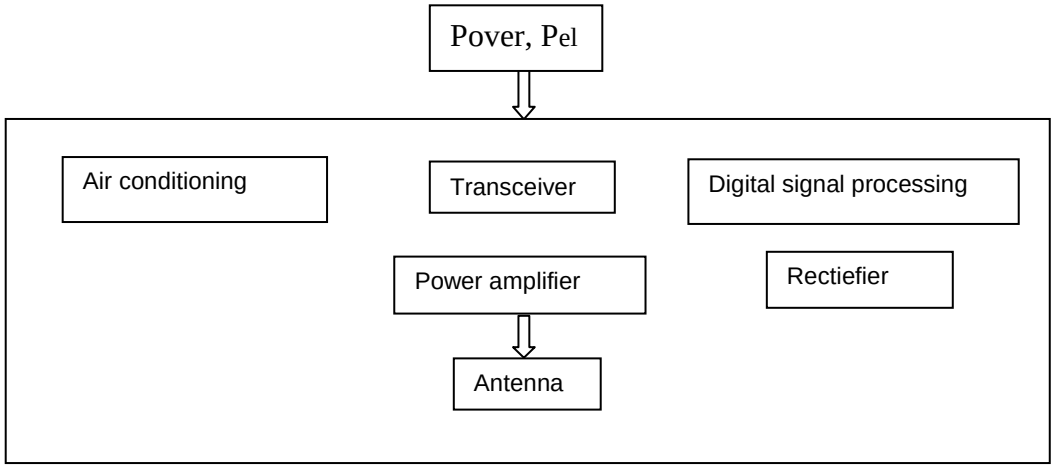


Рис.1. Блок-схема обладнання мікростільникової базової станції.

Після того, як буде знайдена потужність кожного компонента можна буде знайти загальну потужність:

$$P_{el/micro} = P_{el/amp} + P_{el/trans} + P_{el/proc} + P_{el/rect} + P_{el/airco} \quad (3)$$

У таблиці наведено типові енергоспоживання різних компонентів для розглянутих технологій. Ці значення беруться з листів даних різних виробників мережевого устаткування значення, які для мікростільникових та макростільникових мереж дуже схожі, за винятком значення на кондиціонування повітря. Це значення призводить до суттєвого зниження споживання енергії – 60Вт для мікростільнкових, 225Вт для макростільникових базових станцій[1].

Табл.1 Електроспоживання компонентами мікросових базовох станцій.

Equipment		**Value**
Digital signal processing	$P_{el/proc}$	100 W
Power amplifier	η	12%
Transceiver	$P_{el/trans}$	100 W
AC-DC converter	$P_{el/conv}$	100 W
Air conditioning	$P_{el/airco}$	60 W

Деякі параметри будуть мати значення, відмінні від значень для матросового зв’язку, такі як вхідна потужність антени і посилення антени. Уданому дослідженні використаємо типове значення вхідної потужності антени 2Вт, що відповідає 33дБм[1]. Мікростільникова базова станція має лише один сектор, отже використовується всенаправленна антена. Посилення змінюється від 4 до 6 дБ в залежності від технології.

Розглянемо випадок: у приміській зоні вимога покриття 90%, висота мобільних станцій 1,5м, антена мікростільнікової станції на висоті 6м. Мікростільникові станції розміщуються на відкритому повітрі і для мобільних станцій, які всередині приміщення, розглядається з картою бездротового мережевого інтерфейсу (WNIC) для ноутбука[1].

Параметри технологій для мікростільникових базових станцій[1].

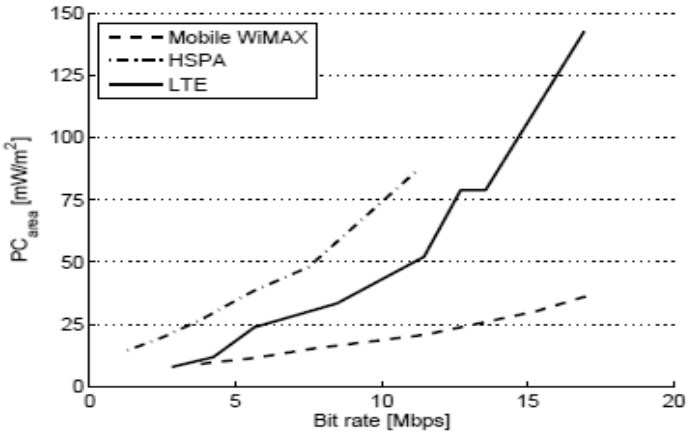


Рис.2. Потужність споживання PCarea за критій площі в залежності від швидкості передачі даних (в Мбіт).

Загалом, рис. 2 показує, що кожна технологія стає менш енергоефективною для більш високих швидкостей передачі даних, як площа збільшується для збільшення швидкості передачі бітів. Чим вище бітрейт, тим вище відношення сигнал-шум. Крім того, більш високий SNR відповідає з меншим діапазоном для того ж потужність Рел, що призводить до більш високого значення для PCarea і, таким чином, більш низьку ефективність використання енергії.

Мікростільникова базова станція споживає близько 376.6W для кожної технології (табл. 1). Однак діапазон R відрізняється між розглянутих технологій. Для бітової швидкості 10 Мбіт, R дорівнює 76,0 м, 37,0 м і 48,0 м для мобільного WiMAX, HSPA і LTE відповідно. Чим вище R для тих же самих результатів Pel в нижчій PCarea і, отже, в більш високій ефективності використання енергії.

Рис.2 показує, що мобільний WiMAX є найбільш енергетично ефективна технологія для швидкості передачі даних вище, ніж 3,8 Мбіт (низька PCarea 20,8 мВт/м2 зі швидкістю 10 Мбіт в порівнянні з 87,6 мВт/м2 і 52,0 мВт/м2 для HSPA і LTE відповідно). Для швидкостей передачі бітів, що розглядаються, Mobile WiMAX працює краще, ніж HSPA і LTE в зв'язку з його більш високим коефіцієнтом посилення антени як на базовій станції і мобільною станцією (табл.2). Крім того, мобільний WiMAX має більш високу ефективну вхідну потужність антени, ніж HSPA.

Швидкості передачі бітів між 2,8 Мбіт і 3,8 Мбіт підтримуються тільки HSPA і LTE. У цьому випадку, LTE є найбільш енергоефективним за рахунок більш високого Ptch Tx (PCarea 2,8 мВт/м2 у порівнянні з 19,7 мВт/м2 для швидкості передачі даних 2,8 Мбіт). Бітові швидкості нижче 2,8 Мбіт підтримуються тільки HSPA (PCarea = 14,5 мВт/м2 протягом 1,3 Мбіт)[1].

Література

1. Modelling the Energy Efficiency of Microcell Base Stations/ Margot Deruyck, Emmeric Tanghe, Wout Joseph and Luc Martens// ENERGY – 2011, 6 ст.

УДК 621.396.1

ИССЛЕДОВАНИЕ ПРОЦЕДУРЫ ПЕРЕДАЧИ ОБСЛУЖИВАНИЯ В БЕСПРОВОДНЫХ СЕТЯХ С УЧЕТОМ ТРЕБОВАНИЙ К МОБИЛЬНОСТИ И НАГРУЗКЕ

Бондаренко Е.И., Кравчук С.А.
Институт телекоммуникационных систем НТУУ «КПИ», Украина
E-mail: ye.bondarenko@gmail.com

Research of handover in wireless networks considering with mobility and load control requirements

It is widely expected that next-generation wireless communication systems will be heterogeneous, integrating a wide variety of wireless access networks. Special interest is focused on combining of cellular networks (GSM/GPRS and WCDMA) and wireless local area networks (WLANs) to provide complementary features in terms of coverage, capacity and mobility support. It is considered that a heterogeneous network of the future will be based on cellular / WLAN interworking and analysis of complex handover traffic rates in the system is one of the most essential issues.

При построении универсальных гетерогенных сетей все большее значение приобретают беспроводные сети связи. Ключевой особенностью таких сетей является поддержание мобильности абонентов. На сегодняшний день известно много различных технологий радиодоступа, положение которых в гетерогенной сети следующего поколения будет только укрепляться. Стремление пользователей к абсолютной свободе порождает множество мобильных сервисов и услуг. Одной из основных процедур по обеспечению мобильности выступает процедура передачи обслуживания (ПОб). Постоянно растущая потребность в большей скорости передачи, обработке большего количества данных с предоставлением максимально возможных показателей качества дает толчок к постоянному совершенствованию и разработке новых сетей и технологий, что в свою очередь приводит к постоянному улучшению механизмов обеспечения мобильности, и как следствие механизмов реализации процедуры ПОб [4].

Разнообразие типов современного трафика и различных сервисов предполагает наличие эффективных механизмов по обеспечению ПОб. Целью данной работы является усовершенствование математических методов анализа процедуры ПОб как альтернативы практическому моделированию, где при их корректном применении можно будет улучшить эффективность управления ресурсами сети в целом.

Каждый с моделируемых сетевых узлов будет представлен в виде системы массового обслуживания для оценки показателей качества QoS, таких как вероятности блокирования вызова, вероятности потери вызова передачи обслуживания и определения приема вызова и распределения ресурсов. Анализ системных характеристик и оценка производительности

взаимодействия в гетерогенных беспроводных сетях будет произведена на основании методов иерархических сотовых сетей.

Большинство предшествующих исследований акцентировали внимание на разработке межсетевых архитектур. Организация сетевого обмена рассматривается с точки зрения выбора доступа, контроля безопасности, управления мобильностью и др. Высоко детализированное моделирование в специальных программных пакетах является очень сложным и не всегда реализуемым, особенно при исследовании разнообразных систем при определении вероятностей редких событий и нахождении значений устойчивых состояний [1].

Именно для преодоления данных ограничений при моделировании следует разработать некоторые аналитические методы для общего анализа интеграции сотовых сетей и локальных беспроводных сетей связи. Главным преимуществом этого подхода будет возможность добавления ряда численных методов по оптимизации сети и избежание ошибок, внесенных каким-либо программным продуктом при моделировании [2].

Как уже упоминалось ранее, работа проводится на основании теории сетей массового обслуживания (СМО), которая является мощным математическим инструментом при оценке производительности многих крупномасштабных инженерных систем и широко применяется в сфере телекоммуникаций. Самая сеть будет представлена в виде группы узлов, каждый с которых представляет собой «услугу». В общем случае абоненты могут появляться и уходить из системы в любом из узлов. Таким образом, клиенты могут свободно входить в систему, выходить из нее, двигаться внутри от одного узла к другому. Причем характер их движения – случайный, то есть они могут двигаться не обязательно по определенным путям, уходить из системы со случайных узлов, возвращаться назад или вообще не покидать систему.

Важным способом оценки мобильности является использование показателя трафика ПОб в процентном соотношении от нового трафика по следующей формуле:

$$\lambda_h = \frac{n}{\mu}\lambda_l = \nu\lambda_l$$

Где, λ_h - показатель трафика ПОб; λ_l – показатель общего количества звонков в соте; ν – параметр, который определяет среднее количество трафика ПОб на один вызов.

WLAN в силу своей зоны работы внутри помещений имеет свойство «низкой» мобильности, в то время как мобильность пользователей в сети сотового покрытия намного выше и в случае их наложения поведения мобильности несколько осложняется. Таким образом несложные математические расчеты представления мобильности в среде сотовой связи несколько усложняются использованием «тяжелых» коэффициентов в выражениях, что заметно усложняет анализ. В качестве решения предложено использование двухступенчатого виперэкспоненциального распределения для аппроксимации времени пребывания пользователей в сети WLAN.

Согласно ему функция плотности вероятности времени пребывания пользователя внутри WLAN определяется:

$$f_{T_r^w}(t) = \frac{a}{a+1}\frac{1}{\frac{1}{a}*\frac{1}{\eta^w}}e^{-a\eta^w t} + \frac{1}{a+1}\frac{1}{a*\frac{1}{\eta^w}}e^{-\frac{\eta^w}{a}t} \qquad a \geq 1, \quad t \geq 0$$

Где a – параметр изменения мобильности; $\frac{1}{\eta^w}$ – численное значение длительности T_r^w нахождения пользователя внутри зоны WLAN.

Исходя из этого выражения большая часть мобильных абонентов $\frac{a}{a+1}$ остается в зоне покрытия сети WLAN на время $\frac{1}{a} * \frac{1}{\eta^w}$, в то время как меньшая часть $\frac{1}{a+1}$ имеет «время жизни» $\frac{1}{a*\frac{1}{\eta^w}}$.

Аналитические методы позволят обеспечить многокритериальную оценку сети и оптимизацию процедур передачи обслуживания в условиях интеграции беспроводных сетей. Адекватность предложенных методов будет проверена программными средствами моделирования и может использоваться для дальнейших исследований, не ограничиваясь показателями мобильности и типом трафика.

Таким образом с помощью применения теории СМО получено модель сети на базе очередей для оценки потоков трафика в гетерогенной беспроводной сети. Для упрощения анализа трафика ПОб была улучшена схема сетевой топологии, предложенная в работе [3], которая позволяет эффективно преобразовывать абстрактные потоки трафика в четкое графическое представление, а затем в решаемую систему уравнений и предложено новый аналитический подход в оценке параметров качества QoS на базе использования Марковских процессов.

Литература

1. R. Srikant and W. Whitt, Simulation run lengths to estimate blocking probabilities, ACM Transactions on Modeling and Computer Simulation, Vol. 6, no. 1, pp. 7-52, January 1996
2. D. E. Everitt, Traffic engineering of the radio interface for cellular mobile networks, Proc.IEEE, vol. 82, no. 9, pp. 1371-1382, September 1994
3. Guozhi Song. Queueing Networks for Vertical Handover: diss..Ph.D.- London, 2009.- 120 pages.
4. Jaydip Sen. “Mobility and Handoff Management in Wireless Networks”, Book Chapter in “Trends in Telecommunications Technologies”, Christos. J. Bouras (Ed.), INTECH Publishers, Croatia, March, 2010. Chapter 22, pp. 457- 484.

УДК 621. 396.1

ТРАНСПОРТНІ БЕЗПРОВОДОВІ МЕРЕЖІ ДЛЯ СИСТЕМ МОБІЛЬНОГО ЗВ'ЯЗКУ 5-ГО ПОКОЛІННЯ

Малецький Д.В., Кравчук С.О.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: DMIAML@ukr.net

Wireless backhaul networks for 5G mobile communication systems

Two typical small cell scenarios are configured to analyze the wireless backhaul traffic. The energy efficiency of wireless backhaul networks is compared in two typical small cell scenarios.

Очікується, що деякі потенційні технології передачі зможуть забезпечити підтримку зростаючих в 1000х об’ємів безпроводового трафіку. MIMO технології прийняті для покращення спектральної ефективності до 10-20 разів в тій самій частотній смузі. Технологія зв’язку на міліметрових хвилях досліджується, щоб бути впровадженою в стільникові мережі, зможе забезпечити частотну смугу більше ніж на 100 МГц. Використання цих технологій призведе до зменшення зони покриття стільників і стане причиною появи мікростільників в 5G мережах. Виникає потреба в повторному перегляді рівнів системи та архітектури. Саме тому, дана тема є актуальною в наш час.

Одним з рішень, для задоволення потреби гігабітного рівня інформаційного трафіку в економічний та екологічний спосіб, є мережа з мікро стільниками, що щільно розміщенні за допомогою малих базових станцій (SBS), які само організовуються, є недорогими і споживають малу потужність. В такому разі виникає проблема, направити масивний транспортний трафік до базової мережі та уникнути сигнального завантаження на вузлах мережі, що зросте в зв’язку з частою передачею обслуговування (ПОб) та погіршеною мобільною надійністю, яка спричинена зростанням ПОб та помилок радіоз’єднання.

Для детального дослідження та порівняльного аналізу пропускної здатності та енергоефективності безпроводових мереж 5G розглядаючи мікростільники і зв’язок за допомогою міліметрових хвиль, запропоновано два рішення. Також проведено оцінку моделі безпроводового транспортного трафіку базуючись на двох рішеннях з різними спектральними ефективностями.

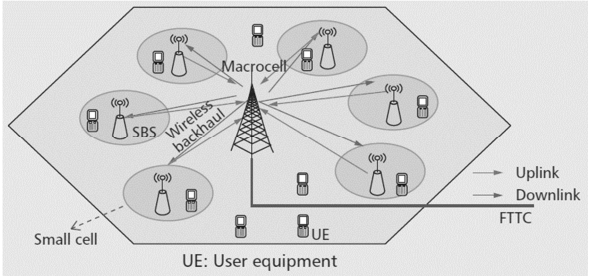


Рис.1 Логічна архітектура центрального рішення.

Перший варіант транспортної мережі, визначений як центральне рішення, представлено на рис.1.

Базова станція в макростільнику (MBS) розташовується в центрі макростільника, а малі базові станції (SBS) рівномірно розподіленні в ньому. Всі SBS налаштовуються на однакову потужність передачі та зону покриття. На рис. 1 трафік бездротової транспортної мережі мікро стільників передається до MBS за допомогою каналу зв'язку в міліметровому діапазоні хвиль, потім об'єднаний «транспортний» трафік направляється з MBS до центральної мережі за допомогою з'єднання «волокно до стільника» (FTTC). Логічні інтерфейси, S1 та X2, які використовуються для направлення транспортного трафіку в центральному рішенні. S1 слугує, як канал для користувацьких даних від підвідного шлюзу до MBS, підвідний шлюз – вхід до центральної мережі. X2 уможливлює взаємний обмін інформацією між мікро стільниками.

Друге рішення для транспортної мережі визначене як розподілене рішення представлене на рис. 2.

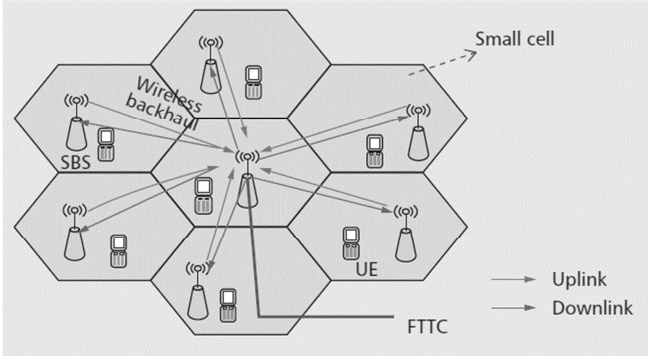


Рис.2 Логічна архітектура розподіленого рішення.

В порівнянні з центральним рішенням на рис.1, в ньому не має MBS, що збирає весь транспортний трафік від мікро стільників і весь трафік транспортної мережі передається до обумовленої SBS, яка з'єднана з базовою мережею з'єднаннями типу «волокно до стільника». На рис. 2 прийнято, що всі SBS рівномірно розподілені по території. Трафік транспортної мережі SBS переданий сусідніми SBS з використанням зв'язку на міліметрових хвилях. Функції логічних інтерфейсів S1 та X2 така ж як і в центральному рішенні.

Більшість трафіку утворюється користувацькими даними. Однак, надлишок транспортного трафіку спричинений протоколами передачі на інтерфейсах S1 і транспортним трафіком про ПОб між сусідніми мікро стільниками є важливою частиною транспортного трафіку. Приймається що всі мікро стільники мають однакову смугу частот і середню спектральну ефективність.

Трафік транспортної мережі в центральному рішенні включає трафік аплінку та даунлінку в макростільнику та в мікростільниках. Прийнято, що трафік транспортної мережі збалансований в кожному мікро стільнику. Загальна кількість мікро стільників в макростільнику обрана як N. Згідно з [1] загальна пропускна здатність аплінку транспортної мережі в центральному рішенні розраховується $TH_{sum-up}^{centra} = N \cdot TH_{small-up}^{centra} \cdot TH_{macro-up}^{centra}$ і даунлінку $TH_{sum-down}^{centra} = N \cdot TH_{small-down}^{centra} \cdot TH_{macro-down}^{centra}$

Як наслідок, загальна пропускна здатність транспортної мережі в центральному рішенні є сума $TH_{sum}^{centra} = TH_{sum-up}^{centra} + TH_{small-down}^{centra}$

В розподіленому рішені, сусідні мікростільники кооперативно направляють трафік транспортної мережі до спеціальної базової станції мікро стільника (SBS). Крім того, не тільки канальна інформація але також дані користувача обмінюються в сусідніх кооперативних SBS. Сусідні об'єднані мікро стільники структуровані в спільний кластер, кількість сусідніх мікро стільників в кластері прийнята рівною К.

Загальна пропускна здатність транспортної мережі розподіленого рішення визначається як

$$TH_{sum}^{dist} = K \cdot (TH_{small-up}^{dist} + TH_{small-down}^{dist}).$$

Розглядаючи пропускну здатність безпроводової транспортної мережі в центральному рішенні, енергетична ефективність центрального рішення як

$$\eta_{centra} = TH_{sum}^{centra} / E_{system}^{centra}$$

Енергетична ефективність розподіленого рішення визначена як

$$\eta_{dist} = TH_{sum}^{dist} / E_{system}^{dist}$$

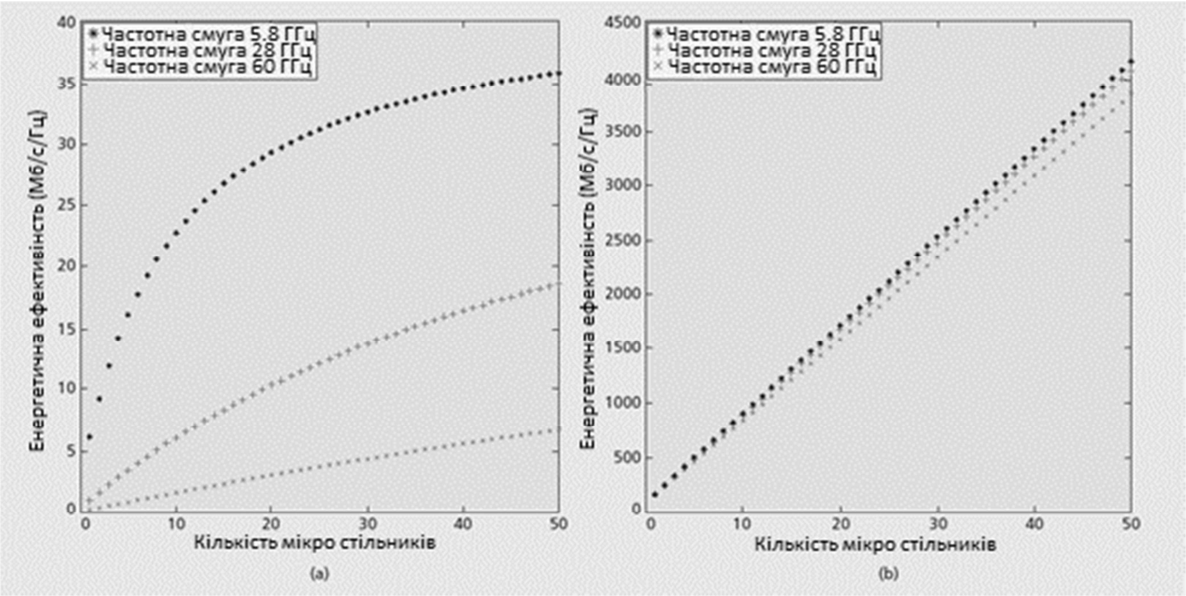


Рис. 3 Енергетична ефективність транспортної мережі з врахуванням кількості мікро стільників для різних частотних смуг: а) центральне та б) розподілене рішення.

Досліджено шляхи розвитку безпроводової транспортної мережі 5-го покоління задля забезпечення високої пропускної здатності та низького енергоспоживання. Два типові способи реалізації з мікро стільниками створені для аналізу безпроводового транспортного трафіку в майбутніх 5G мережах. Числові результати свідчать про те, що розподілене рішення має вищу енергоефективність ніж центральне в безпроводових транспортних мережах 5G.

Література

1. 5G Wireless Backhaul Networks: Challenges and Research Advances / X.Ge, H. Cheng, M. Guizani, T. Han. // IEEE Network. – 2014.

УДК 621.391

ИССЛЕДОВАНИЕ ПРОЦЕССА ПЕРЕДАЧИ ОБСЛУЖИВАНИЯ В МИКРОСОТОВЫХ СЕТЯХ СТАНДАРТА LTE С ИСПОЛЬЗОВАНИЕМ ИНТЕРФЕРЕНЦИОННОЙ КООРДИНАЦИИ

Рак Р.И., Кравчук С.А.
Институт телекоммуникационных систем НТУУ «КПИ», Украина
E-mail: foxter222@ukr.net

Research of handover in micro cellular LTE networks with the interference coordination

In this article is proposed an enhanced inter cell interference coordination (ICIC) mechanism based on Multi Armed Bandit (MAB) approach that aims at maximizing throughputs of the attached users and their handover performances evaluated through 3GPP Mobility Robustness Optimization (MRO) indicators.

Для построения мобильных сетей 4G и дальнейшего их развития до 5G получил развитие стандарт LTE (Long Term Evolution). На сегодня, согласно данных Global mobile Suppliers Association (GSA) уже запущено 480 сетей стандарта LTE в 157 странах. Не смотря на такое распространение данной технологии, координация интерференции между сотами ICIC (Inter Cell Interference Coordination) и оптимизация передачи обслуживания остаются двумя основными техническими проблемами, которые препятствуют эффективному развертыванию LTE-сетей [1]. В особенности это касается случаев плотного развертывания небольших сот (микросот) с целью решения проблемы обслуживания постоянно растущих объемов трафика и охвата зон с недостаточным покрытием.

На производительность передачи обслуживания оказывает большое влияние интерференция, особенно межсотовая, которая встречается при выполнении передачи обслуживания НО (HandOver) на границах сот, где уровень помех является наиболее критичным. В зависимости от уровня интерференции, воспринимаемого пользователем на краю соты, в ситуации касающейся передачи обслуживания, важным аспектом является умение правильно и вовремя переключиться на обслуживание соседней базовой станции (БС). Если на краю соты присутствует интерференция высокого уровня, крайне важно инициировать передачу обслуживания иначе, она может быть затруднена. Данная ситуация будет считаться в качестве передачи обслуживания с запозданием. С другой стороны, для того же расположения абонента, если уровень интерференции очень низкий, решение переключиться на другую БС, вероятно, может быть слишком ранним и приведет к ошибочным решениям касательно инициации передачи обслуживания или к выбору неправильной целевой соты. В этом случае, становится очевидным, что совместная настройка и оптимизация ICIC и процесса НО – важная техническая задача, требуемая решения.

До решения данной задачи были проведены несколько исследований, которые показывают взаимосвязь между ICIC-механизмами и передачей обслуживания в сетях стандарта LTE. В работе [2] представлено влияние схемы

ICIC на процесс HO, которое с количественной точки зрения оценивалось числом передач обслуживания и уровнем блочных ошибок BLER (Block Error Rates). Этот метод хорошо подходит для стандартного развертывания сот (макросот), но в то же время он не является оптимальным для развертывания микросот, где выдвигаются более жесткие требования к самоорганизации сети. В [3] было проанализировано взаимодействие между HO и ICIC в микросотовых LTE-сетях, также было оценено влияние управления межсотовой интерференции на производительность передачи обслуживания для различных конфигураций.

В данной работе предлагается математическая модель, которая учитывает в явном виде ключевые показатели эффективности процесса передачи обслуживания внутри механизма ICIC. Метрики передачи обслуживания для соответствия стандартизации рассматриваются как стандартные показатели оптимизации надежности мобильной сети MRO (Mobility Robustness Optimization), представленных в 3GPP [4]. Необходимо, чтобы существовала возможность переконфигурирования механизма ICIC таким образом, чтобы минимизировать интерференцию на границах сот к допустимому уровню, после чего будут выполнены цели MRO: уменьшение количества разорванных вызовов, приведение к максимально возможному минимуму вероятности отказа передачи обслуживания, уменьшение избыточных HO.

В работе используется модель, где вся доступная полоса частот делится на равные поддиапазоны. Эти поддиапазоны обозначены как $\{SB_i\}_{i=1}^{N}$, где N – общее количество поддиапазонов. В каждый момент времени итерации t БС должна выбрать поддиапазон для передачи. Так как рассматривается плотное развертывание микросот, то необходимо, чтобы процесс координации интерференции проходил в автономном режиме.

Для этой цели предлагается использовать алгоритм верхнего доверительного предела [5], который является методом обучения с подкреплением и используется для решения задачи «многорукого бандита» MAB (Multi Armed Bandit). Этот алгоритм имеет преимущество в вычислительном плане, поскольку он не требует предварительных знаний о распределении выигрыша. Единственное условие, необходимое для вычисления верхней границы потерь состоит в том, что выигрыш находится в диапазоне [0, 1]. В исследуемом случае это условие реализуется путем деления функции выигрыша по связанному максимуму.

При таком подходе используется функция принятия решений, которая однозначно определяет следующий поддиапазон доступный для БС. На каждой t итерации базовая станция выбирает $SB_{g,t}$, который идентифицированный как «жадный» поддиапазон g, при этом максимизируя значение функции принятия решения, рассчитанное во время t для каждого поддиапазона, идентифицированного индексом i: $DF_{i,t}$.

$$SB_{g,t} = argmax_{1 \le i \le N} \tag{1}$$

Функция принятия решений формулируется следующим образом:

$$DF_{i,t} = \mu_{i,t} + \sqrt{\frac{2 \times \log\left(\sum_{i=1}^{N} n_{i,t}\right)}{n_{i,t}}}, \tag{2}$$

где: $\mu_{i,t}$ – среднестатистическая функция выигрыша поддиапазона i в

момент времени *t*. Этот параметр указывает на производительность базовой станции, которая осуществляет передачу сигналов в поддиапазоне *i*; $n_{i,t}$ – параметр, показывающий сколько БС работало в поддиапазоне *i* до момента времени *t*. Параметр N соответствует общему количеству поддиапазонов, которые корректируются динамично в соответствии с показателями MRO (3).

В методике MAB число поддиапазонов N может увеличиваться или уменьшаться детерминированным способом на основе показателей MRO, таких как отношение сигнал/шум (SINR). При этом нужно учитывать возможность возникновения НО с запозданием и, в результате, разрыва процесса передачи обслуживания. Была предложена следующая формула:

$$N=\begin{cases} N+1 \; если \\ НО_{зап.} > Порог.знач.1 \; либо \; SINR < Порог.знач.2 \\ N-1 \; если \\ Total_{failures} < Порог.знач.3 \end{cases} \quad (3)$$

вместе с: $Total_{Failures} = НО_{зап.} + НО_{ран.} + НО_{непр}$.

В действительности, число поддиапазонов увеличивается в двух случаях: низкое значение отношения SINR по всей зоне покрытия соты; большое количество НО с опозданием, которое соответствует высокому уровню интерференции, воспринимаемой пользователями в области передачи обслуживания.

Таким образом, каждой соте предоставляется больше вариантов для выбора необходимого поддиапазона, что уменьшает риск повторного использования одних и тех же ресурсов и минимизирует влияние интерференции на абонентов. Также стоит отметить, что в случае низкой интенсивности отказов передачи обслуживания можно утверждать, что уровень интерференции, воспринимаемый на границах сот, не есть критическим, из-за чего можно получить выигрыш за счет увеличения размера дозволенной пропускной способности соты (уменьшив количество «рук»), что в результате приводит к более высокой пользовательской пропускной способности.

Литература

1. Stefania Sesia, Issam Toufik, Matthew Baker, LTE the UMTS long term evolution, Second Edition, Wiley.
2. Рак Р.І., Кравчук. С.О. Покращення характеристик передачі обслуговування в мережі LTE за допомогою інтерференційної координації. Проблеми телекомунікацій : 8-а Міжнар. наук.-техн. конф., 16-19 квіт. 2014р. : матеріали конф. – К., 2014. – С. 148–150.
3. V. Capdevielle, A. Feki and E. Sorsy, Joint Interference Management and Handover Optimization in LTE Small Cells Network, IEEE ICC12, International workshop on Small Cell Wireless Networks, June 15th, 2012.
4. 3GPP TS 36.423, Evolved Universal Terrestrial Radio Access Network (E-UTRAN) ; X2 application protocol (X2AP) (Release 9), 9.4.0 ed., 2010.
5. P. Auer, N. Cesa-Bianchi and P. Fischer, Finite time Analysis for the Multi-armed Bandit Problem, Machine Learning, 47, 235-256, 2002.

УДК 621. 396.1

ПІДТРИМКА МОБІЛЬНОСТІ В ГЕТЕРОГЕННИХ МЕРЕЖАХ ШИРОКОСМУГОВОГО ДОСТУПУ

Казачінер К.А., Кравчук С.О.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: kazachinerkiril@gmail.com

Mobility support in heterogeneous wireless networks

The solution to support applications who are mobility-aware and those who are not. Using the context of cross-layer information for enhances handovers decisions, transport performance and media adoption.

На даний час широке поширення набули безпроводові мережі абонентського доступу, що базуються на сучасних радіотехнологіях та мережних протоколах. Необхідною умовою подальшого впровадження безпроводових мереж є підтримка ними мобільності, тобто безперервної передачі обслуговування. За допомогою використання мобільності користувач має можливість переключатись між пристроями, мігрувати крізь сесії та отримувати одні й ті ж персональні сервіси.

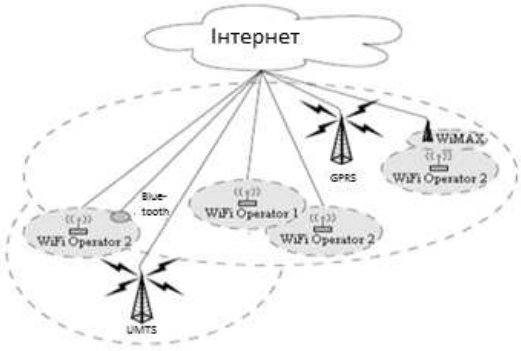


Рис. 1 Безпроводовий доступ до гетерогенної мережі Інтернет.

Дана робота представляє рішення з управління мобільністю для підтримки застосувань, які можуть враховувати мобільність. Для управління мобільністю в гетерогенному середовищі необхідно використовувати подвійне значення IP-адреси в якості ідентифікатора кінцевої точки та ідентифікатора місцезнаходження. Прикладний рівень мобільності використовує ідентифікатор без прив’язки до IP кінцевих точок (наприклад, user@realm), у той час як мережевий рівень мобільності використовує фіксовані домашні IP-адреси в якості ідентифікатора кінцевої точки. Рішення ідентифікатора кінцевої точки для тимчасового одноадресного IP адресу, як ідентифікатора місцеположення, потребує підтримки системи управління мобільністю. Дана робота пропонує систему підтримки мобільності, яка об'єднує переваги рівня застосувань SIP-мобільності з мережним рівнем MIP-

мобільності. Інформація з застосування підходу поперечного рівня забезпечує контекст для мобільної адаптації. Такий контекст покращує передачу обслуговування, транспортну та медійну ефективність. Мережевий рівень мобільності підтримує програми з визначення місцезнаходження «на-вимогу» для початкового налаштування сесій. В даній роботі пропонується система обміну інформацією поперечного-шару, що підвищує адаптацію мобільності (наприклад, рішення передачі обслуговування, адаптивні якості відео і т.д.).

Система підтримки мобільності складається з мобільної підтримки агентів (MSA) в домашній та в зовнішній мережі. HMSA надає послуги домашнього агента MIP і SIP перенаправлення/реєстрації сервера. FMSA надає послуги сповіщення агента та розподілу IP-адреси. Вся функціональність може підтримуватися в одному сервері. Щоб включити прямий зв'язок між кінцевими хостами, домашній хост вимагає суміщену адресу виходу (CCoA) в зовнішній мережі.

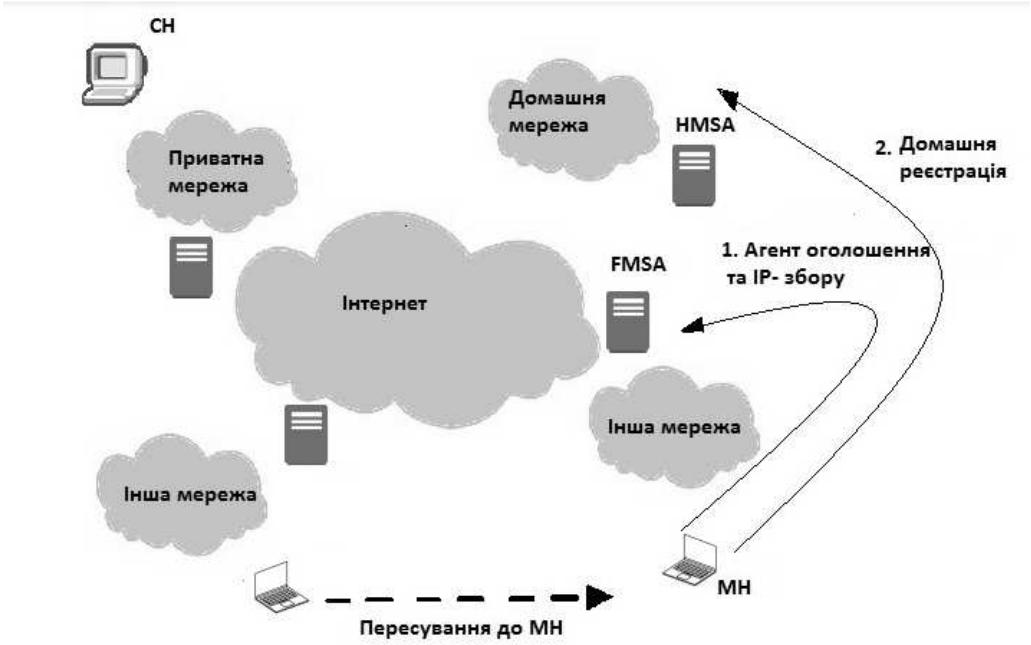


Рис. 2 Архітектура підтримки мобільності.

Управління мобільністю підтримується як на мережевому так і на прикладному рівні. Ми обираємо для опису мобільності як мережевий рівень так і прикладний, в той час коли фактичний вибір приймається додатком вимог у реальному часі. Коли домашня адреса використовується в якості IP джерела, мережний рівень буде обробляти мобільність за замовчуванням і, якщо додаток обирає обробку мобільності самостійно , він повинен використовувати CoCA в якості джерела IP.

Обмін інформації поперечного рівня підтримує сервіси поділу послуг , що базується на вимогах вищих рівнів. Якщо пристрій має багато безпроводових мережних інтерфейсів, вибір відповідного інтерфейсу може базуватися на потребах користувачів або вимог мультимедійних додатків.

Наприклад, коли додаток у поєднанні з жорсткими вимогами затримки ,інтерфейс WLAN може бути використаний для кращої пропускної здатності. Але якщо низькі вимоги затримки є допустимими, пристрій може переключитися на інтерфейс GPRS. Мобільність, пов'язана з контекстом може бути обмінена між рівнями, щоб зробити адаптацію мобільності більш ефективною. Параметри канального рівня такі як рівень сигналу, початок передачі обслуговування і здійснення події можуть бути використані, щоб зробити процес хендоверу на мережевому рівні більш ефективним. Параметри канального рівня, такі як втрата пакетів та BER(кількість помилок) також можуть бути використаний для гарної настройки продуктивності на транспортному рівні (наприклад, ретрансляція та відхід) і для прийняття на рівні додатків (наприклад медійне кодування та оцінка передачі).

Рис.3 Обмін інформацією поперечного рівня

Отже, у даній роботі розглянуто комплексне рішення , яке поєднує у собі використання переваг різних рівнів SIP та MIP-мобільності. Таке рішення дозволяє додатку обрати метод мобільності для використання на основі реального часу або з вимогами не для реального часу. Зазначений вище опис системи обміну інформацією поперечного шару дає якісні показники у адаптації мобільності, що впливає на рішення хендоверу, якості відео та ін.

Література

1. Mobility Management for multiple diverse applications in heterogeneous wireless networks - Robert Brännström, Ruwini Kodikara, Christer Åhlund, Arkady Zaslavsky.

УДК 621.39

ПЕРЕДАЧА ОБСЛУГОВУВАННЯ В WIMAX/LTE НА БАЗІ IMS-АРХІТЕКТУРИ

Семендяк Є.С., Кравчук С.О.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: semendyak@gmail.com

An IMS-based integration architecture for WiMAX/LTE handover

To provide users with always-on connectivity, researchers have tackled the issue of the integrating beyond 3G networks such as 3GPP Long Term Evolution LTE and non-3GPP networks. In this context, was proposed an integration architecture for WiMax and LTE access technologies based on EPC as core network and IMS for service provisioning.

Стрімкий розвиток безпровідних мобільних телекомунікаційних систем призвів до виникнення нових технологій зв’язку з різноманітними перевагами, але на рівні з перевагами виникають і своєрідні недоліки.

Для розв’язання даної проблеми часто приходять до своєрідного рішення — використання різних технологій для зв’язку в різних умовах роботи, що в свою чергу, за умови, що ці технології компенсують недоліки одна одної.

На даному етапі розвитку мобільних технологій задля задоволення потреб мобільних користувачів бездротових широкосмугових мереж, було розроблено дві технології для передачі голосу, даних, відео та мультимедіа послуг на мобільних пристроях на високих швидкостях за дешевими тарифами: WiMAX і LTE.

WiMAX є системою бездротовою зв'язку, яка може забезпечити широкосмуговим доступом користувачів з великою площею покриття. Це покращує WLAN (IEEE 802.11), розширюючи безпровідний доступ до WAN (Глобальна Мережа), чи MAN (Міська Мережа). Технологія LTE розвинулась з таких стільникових технологій, як UMTS/HSDPA для задоволення зростаючих потреб в високошвидкісній передачі даних і підвищення мобільності кінцевих пристроїв. LTE спрямована на забезпечення основних IP послуг, гнучкого використання спектру, зниження енергоспоживання і просту мережеву архітектуру з доступними інтерфейсами.

Одна з проблем, пов'язаних з інтеграцією мобільних мереж WiMAX і 3GPP виникає з їх відмінності з точки зору автентифікації, авторизації та обліку (AAA процедур), контролю якості обслуговування (QoS механізми) та мобільності протоколів. Вважається, що архітектура мережі WiMAX — LTE має мати вигляд двох сот, що перекривають одна одну, одна це мережа мобільного WiMAX, що обслуговується базовою станцією і LTE сота, що обслуговується вузлом e-Node B. Тим не менш, зв'язок між додатковими вузлами (що беруть участь в інтеграції) та Мобільною Станцією MS збільшує непродуктивні витрати на сигналізацію і вводить додаткову інформацію, яка повинна бути збережена в вузлі збереження і встановлення функції доступу

до мережі ANDSF.

Інші архітектури інтеграції розглядають IP Multimedia Subsystem IMS в якості перспективного рішення для інтеграції 3GPP і не-3GPP мережі, так як система IMS пропонує необхідне міжмережеве середовище незалежно від будь-якої технології доступу з протоколом SIP (Session Initiation Protocol), що розглядається як ключовий протокол сигналізації IMS. З іншого боку, для управління мобільністю МС в рамках інтегрованої архітектури також вже були продумані такі протоколи мобільності, як Mobile IP (MIPv6) і Proxy-MIP (PMIPv6), що дозволяють мобільним пристроям працювати в іншій мережі, однак ці протоколи відзначаються значною затримкою при передачі обслуговування. Тому для вирішення даної проблеми, було запропоновано використання швидкого хендоверу для Mobile IPv6 (FMIPv6), але даний вид хендоверу, у випадку вертикальної передачі обслуговування між Long Term Evolution (LTE) та іншими видами мереж доступу, такими як FPMIPv6 не може забезпечити надійні безшовні операції VHO. Щоб вирішити проблему вертикальної передачі обслуговування, були запропоновані методи, що використовують поєднання MIP і SIP в мережі IMS з метою скорочення затримки.

Основні вимоги для взаємодії, які повинні бути прийняті до уваги, являються:

- архітектура, що реалізує співіснування обох технологій в мережі all-IP;

- здатність MS виконати передачу обслуговування з мінімальною затримкою і мінімальними витратами сигналізації.

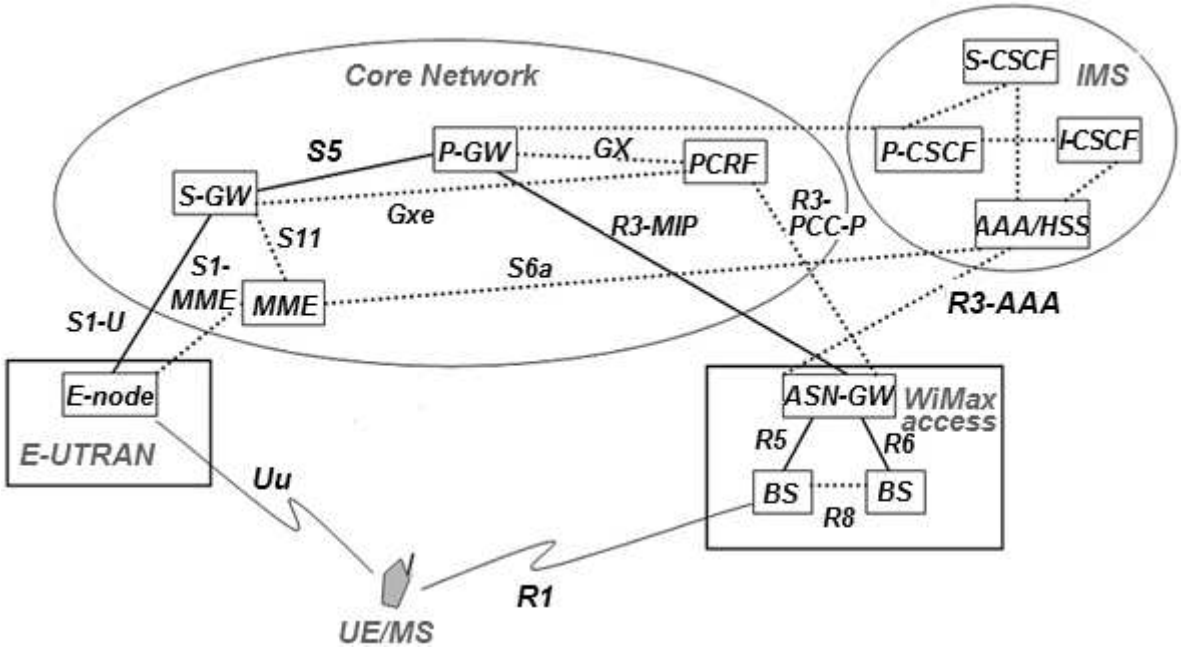


Рис.1 Архітектура інтеграції WiMAX – LTE на базі IMS.

При розгляді питання інтеграції WiMAX-LTE, також слід розглядати процес VHO з точки зору забезпечення безшовної і прозорої мобільності для користувачів роумінгу між різними мережами доступу. IMS-рішення для

мереж WiMAX і 3GPP вирішує проблему безшовного VHO і підтримки QoS з використанням комбінації протоколів MIP і SIP. MIP використовується в якості протоколу управління мобільністю для забезпечення прозорої мобільності вище протоколу мережевого рівня і ініціювання сеансу SIP, який використовується для узгодження сеансу зв'язку під час VHO для забезпечення мобільних користувачів безшовною передачею обслуговування.

Запропонована архітектура інтеграції показана на рис. 1. WiMAX і LTE мережі підключаються до загальної базової мережі EPC. Технологія доступу LTE підключається через шлюз обслуговування (S-GW), в той час, як non-3GPP технологія доступу WiMAX підключається через шлюз мережі з комутацією пакетів даних (P-GW). IMS буде пропонувати необхідне середовище організації мережевого обміну незалежно від будь-якої технології доступу. Базовою мережею є EPC-мережа, яка підключається до IMS через P-CSCF. IMS буде взаємодіяти з сигнальної частиною EPC через Proxy Call Session Control Plane P-CSCF. P-CSCF є точкою входу IMS, яка буде взаємодіяти з P-GW в базовій мережі. S-CSCF є обслуговуючим вузлом, який несе відповідальність за управління сеансом. I-CSCF це опитуючий вузол, який відповідає за функціональні можливості проксі. S-GW, це точка, де об'єднуються канали передачі даних від мереж LTE і 3GPP. AAA / HSS відповідає за центральну базу даних і користувальницьких профілів, таких як політики QoS. MME це точка функції контролю, яка відповідає за мобільність, автентифікацію і безпеку. Вона безпосередньо підключена до контрольної точки HSS / AAA в мережі IMS для контролю відповідності профілю користувача до параметрів QoS в мережі LTE. ASN є шлюзом WiMAX, де політика QoS реалізуються таким чином: він буде взаємодіяти з HSS / AAA-сервером в мережі IMS, з одного боку, і також з'єднаний з P-GW для передачі даних в транспортній мережі частині з іншого боку.

Архітектура дозволить мобільним користувачам виконувати передачу обслуговування WiMAX на LTE або навпаки плавно через мережу IMS з використанням протоколів MIP і SIP, які використовуються для безшовної сигналізації. Безшовної сигналізація буде виконана між P- GW і P-CSCF для управління передачею обслуговування.

Література

1. Tara A. Yahiya, Hakima Chaouchi, On the integration of LTE and mobile WiMAX networks, in: IEEE 19th International Conference on Computer Communications and Networks, ICCCN, 2010.
2. P. Taaghol et al., Seamless integration of mobile WiMAX in 3GPP networks, Communications Magazine, IEEE 46 (2008) 74–85.
3. W. Song et al., Improvements to seamless vertical handover between mobile WiMAX and 3GPP UTRAN through the evolved packet core, Communications Magazine, IEEE 47 (2009) 66–73.
4. А.Л. Гельгор Е.А. Попов - Технология Lte Мобильной Передачи Данных [Електронний ресурс] // Режим доступу до ресурсу: http://www.cee.spbstu.ru/Polozhintsev/popov3.pdf.

УДК 004.89

МОЖЛИВОСТІ ЗАСТОСУВАННЯ «ХМАРНИХ» ТЕХНОЛОГІЙ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Кравчук С.О., Міночкін. Д.А., Рибак О.О.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: alex96.rybak@gmail.com

Possibility of “cloud” technology usage in telecommunication systems

The approaches of modern distributed systems construction are presented. Main "cloud" service architectures are discussed. The analysis of the distributed “cloud” systems usage for development of the future wireless telecommunication systems is conducted.

Хмарні обчислення (Cloud Computing) є технологією обробки даних, в якій комп’ютерні ресурси і служби стають доступні користувачеві в якості веб-сервісу. Технологія «хмарних» обчислень дозволяє задовольнити в тій чи іншій мірі інформаційні потреби підприємства чи окремого користувача зовнішніми провайдерами. В основі Cloud Computing лежать декілька підходів [1]:

- доступність через Інтернет. Хмара видає себе за звичайний сервер в мережі;
- віртуалізація. Завдяки цьому підходу користувач може отримати потрібний йому ресурс. Забезпечення виділення ресурсу користувачеві здійснюється приховано, за стінами віртуальних машин;
- простота і стандартність. При роботі з «хмарою» немає необхідності створювати складні конфігураційні файли. Все, що пропонується всередині хмари, доступно через прості виклики API та протоколи, наприклад, так званий протокол REST (Representational State Transfer – «передача репрезентативного стану»), за допомогою якого всі операції над даними можна робити через http-запити.

Для подальших досліджень та розробки сучасних телекомунікаційних систем необхідно провести аналіз області застосування таких систем.

Основними напрямками «хмарних» послуг є [2]:

- платформа як сервіс PaaS (Platform as a Service);
- послуги інформаційної інфраструктури IaaS (Infostructure as a Service);
- послуги застосувань SaaS (Software as a Service).

Також, можуть надаватися такі послуги, як «робоче місце як в сервіс» WaaS (Workplace as a Service), «апаратура як сервіс» HaaS (Hardware as a Service), «комунікації як сервіс» CaaS (Communication as a Service).

PaaS – це обчислювальна платформа, яка дозволяє створювати веб-додатки. Така платформа забезпечує послуги для розробки, тестування, розгортання і підтримки додатків в інтегрованому середовищі розробки. PaaS доцільно застосовувати, коли кілька розробників будуть працювати над створенням проекту або якщо інші зацікавлені користувачі повинні взаємодіяти з процесом розробки.

IaaS – це надання програмно-апаратних ресурсів, що забезпечує віртуалізацію обчислювальних ресурсів через Інтернет. Складається з трьох основних компонентів – апаратне забезпечення (сервери, системи зберігання даних, клієнтські системи, мережеве обладнання), операційні системи та системне програмне забезпечення (засоби віртуалізації, автоматизації, основні середовища управління ресурсами), і сполучне програмне забезпечення для управління

апаратним і програмним забезпеченням. Віртуалізоване середовище надається IaaS на базі деяких серверів, об'єднаних в кластери. Користувачу надається віртуальна машина, яка працює на системах провайдера, всередині якої є всі можливості для установки спочатку операційної системи, а потім і налаштування програмного забезпечення.

SaaS - підтримує розповсюдження програмного забезпечення з конкретними вимогами. Користувачі можуть використовувати програми та інформацію віддалено через Інтернет і оплачувати тільки за ті ресурси, що були використані. SaaS може бути розгорнутий безпосередньо на IaaS або PaaS.

Одним з перспективних напрямків використання хмарних обчислень є застосування їх для побудови сучасних мобільних телекомунікаційних мереж. На сьогоднішній день до хмарної обчислювальної системи отримують доступ все більше користувачів, які мають смартфони та планшети. Саме хмара в мобільному середовищі породила новий термін «мобільні хмарні обчислення» MCC (mobile cloud computing) [3], які використовують потужну платформу хмарних обчислень для ефективного рішення завдань по зберіганню даних, керуванню та синхронізації, тощо.

З іншого боку, такі потужні технології можуть бути корисними для мереж радіо доступу RAN (radio access networks), що призвело до появи нової концепції хмарних мереж радіодоступу C-RAN (cloud radio access networks) [4]. Хмарна мережа радіодоступу передбачає перехід від розподіленої до централізованої інфраструктури для обробки інформації та керування.

У порівнянні з базовими станціями (BS) традиційних стільникових мереж, BS в C-RAN спрощені, тому що обробка сигналів і прийняття рішень в більшості випадків відбувається в хмарі безпроводової мережі (Рис. 1). BS підключені до хмари безпроводової мережі за допомогою опорних транспортних мереж. Для забезпечення передачі даних в умовах значних затримок використовується спліт-TCP (split-TCP).

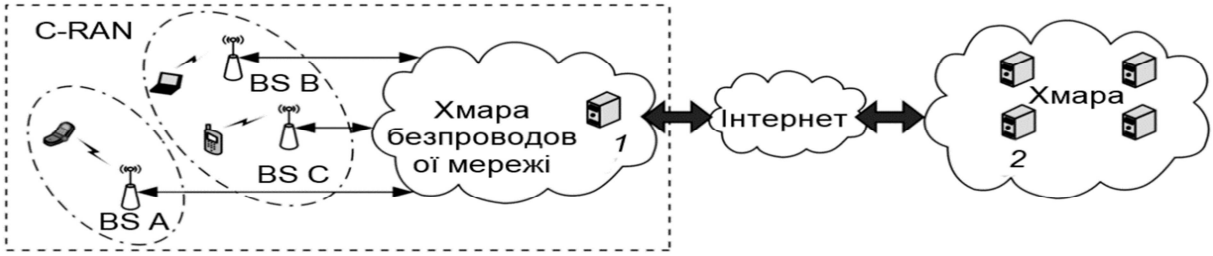


Рис. 1 Хмарна мережа радіодоступу в середовищі MCC:
1 – спліт-TCP проксі (split-TCP proxy); *2* – внутрішній сервер.

Спліт TCP (Split TCP), як правило, використовується для вирішення проблем протоколу TCP з великим значенням часу проходження RTT (round-trip time). Клієнт встановлює TCP-з'єднання з найближчим спліт-TCP проксі сервером, а TCP проксі, в свою чергу, підтримує постійне з'єднання.

З точки зору архітектури, необхідно мати спліт-TCP проксі на краю хмари безпровідної мережі. Проксі сервер може бути реалізований в шлюзі еволюції системної архітектури SAE-GW (system architecture evolution gateway) в LTE-системі, тому що потоки даних користувача тунелюються через SAE-GW перед відправкою до Інтернет [5].

Рис. 2 Логічні стеки протоколів мережних об'єктів: центрів обробки даних, спліт-TCP-проксі і мобільного користувача.

На рис. 2 показано логічний зв'язок мобільних пристроїв, безпроводової мережної хмари і внутрішніх серверів. TCP-потоки передаються з мобільних пристроїв до внутрішніх серверів в хмарі. Хмара безпровідної мережі динамічно управляє безпроводовою мережею за допомогою TCP-проксі, який розташований в хмарі безпроводової мережі, і розбиває з'єднання з кінця в кінець між користувачем і внутрішнім сервером на два з'єднання, а також підтримує постійний зв'язок між собою і внутрішнім сервером. Управління включає в себе розподіл швидкості передачі даних і конфігурацію топології, за допомогою якої можлива кооперація декількох BS. Наприклад, на рис. 1 BS B і C утворюють кластер для спільного обслуговування мобільних користувачів, а BS A сама обслуговує інший кластер. У середині кластера сигнали обробляються спільно, так що інтерференція радіосигналів відсутня.

Таким чином, проведене дослідження показує можливість застосування технології розподілених обчислень для побудови сучасних високопродуктивних безпровідних телекомунікаційних систем, що дозволить зменшити витрати на розгортання та підтримку таких систем для операторів зв'язку.

Література

1. A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches / H. T. Dinh et al. // Wireless Communications and Mobile Computing, 2011.
2. Петренко А.І. Хмарні і грід-обчислення для е-науки // Міжнародна конференція «Кластерні обчислення», Київ, Інститут кібернетики ім. В.М. Глушкова НАН України, 12 - 14 Червня 2012. – С. 123–129.
3. Cai Y., Yu F. R., Bu S. Cloud Computing Meets Mobile Wireless Communications in Next Generation Cellular Networks // IEEE Network. – 2014. – № 9/10. – P. 1–6.
4. CloudIQ: A Framework for Processing Base Stations in a Data Center / S. Bhaumik et al. // Proc. ACM Mobicom'12, (Istanbul, Turkey), 2012.
5. Farkas V., Hder B., Novczki S. A Split Connection TCP Proxy in LTE Networks // Information and Communication Technologies. Vol. 7479 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2012. - P. 263–74.

УДК 621.391

ВИКОРИСТАННЯ СЕРВІСУ DBAAS ПЛАТФОРМИ OPENSTACK ДЛЯ СТВОРЕННЯ БАЗ ДАНИХ ДЛЯ ОПЕРАТОРІВ МОБІЛЬНОГО ЗВ'ЯЗКУ

Кибенко А.В., Міночкін Д.А.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: endryu-kibenko@outlook.com

Usage of DBaaS service of OpenStack platform for creating of databases for mobile operators

OpenStack software conceptual architecture is considered and essence of its main elements is revealed. DBaaS(Database-as-a-Service) service is represented based on the Trove model and its main functional options is described.

Згідно з даними IDC, в 2014 році ринок «хмарних» послуг IaaS/SaaS виріс на 47% до $8,5 млн, а в 2015 році ще на 30% і перевищив позначку в $10 млн. Найбільшими споживачами «хмарних» послуг в Україні, є торгові компанії, на які припадає 26-28% від усього обсягу спожитих послуг. На другому місці банки, які є одними з найбільших споживачів IT-ринку (їх доля 23-25%). Отже, «хмарні» технології стають зручним інструментом в плані фінансового ризику і скорочення витрат [1].

Термін «хмарні обчислення» можна застосувати для будь-яких сервісів, які
надаються через мережу Інтернет. Мета «хмарних обчислень» зводиться до надання кінцевим користувачам віддаленого доступу до послуг і додатків через Інтернет.

Всі Інтернет-послуги, також відомі як «хмарні послуги», розділяють на 3 основні категорії [2]:

- IaaS (інфраструктура як сервіс) – тобто користувач отримує «чистий» екземпляр віртуального серверу з унікальною IP-адресою.
- PaaS (платформа як сервіс) – користувач отримує вже готову до роботи віртуальну платформу, зі встановленим ПЗ.
- SaaS (програмне забезпечення як сервіс) – користувач має можливість користуватись ПЗ віддалено через Інтернет.

Тому, необхідно провести аналіз можливості використання «хмарних» технологій для модернізації інфраструктури оператора мобільного зв'язку.

На даний момент існує дуже багато програмних продуктів для створення «хмарної» інфраструктури, які мають різний функціонал та підтримують створення різних типів хмарних послуг. Однак, для операторів зв'язку найбільш вигідним є перенос фізичної архітектури та сервісів в «хмару». Отже, для них доцільно використовувати IaaS хмару, на базі якої можливо розгорнути інші типи послуг.

Одним із інструментів для побудови IaaS хмари може бути комплекс вільного ПЗ для створення обчислювальних сервісів та хмарних сховищ

OpenStack, який складається з наступних компонентів [3]:

- Nova – засіб управління гіпервізорами.
- Swift – сховище «об’єктів» даних.
- Glance – сховище образів віртуальних машин.
- Horizon – веб-інтерфейс управління.
- Keystone – забезпечує автентифікацію і авторизацію для всіх OpenStack послуг.
- Neutron – засіб управління мережевою інфраструктурою.
- Cinder – сховище блоків даних.
- Heat – система автоматизації хмарних додатків.
- Ceilometer – інструмент моніторингу.

На рис.1 зображена концептуальна архітектура комплексу ПЗ OpenStack.

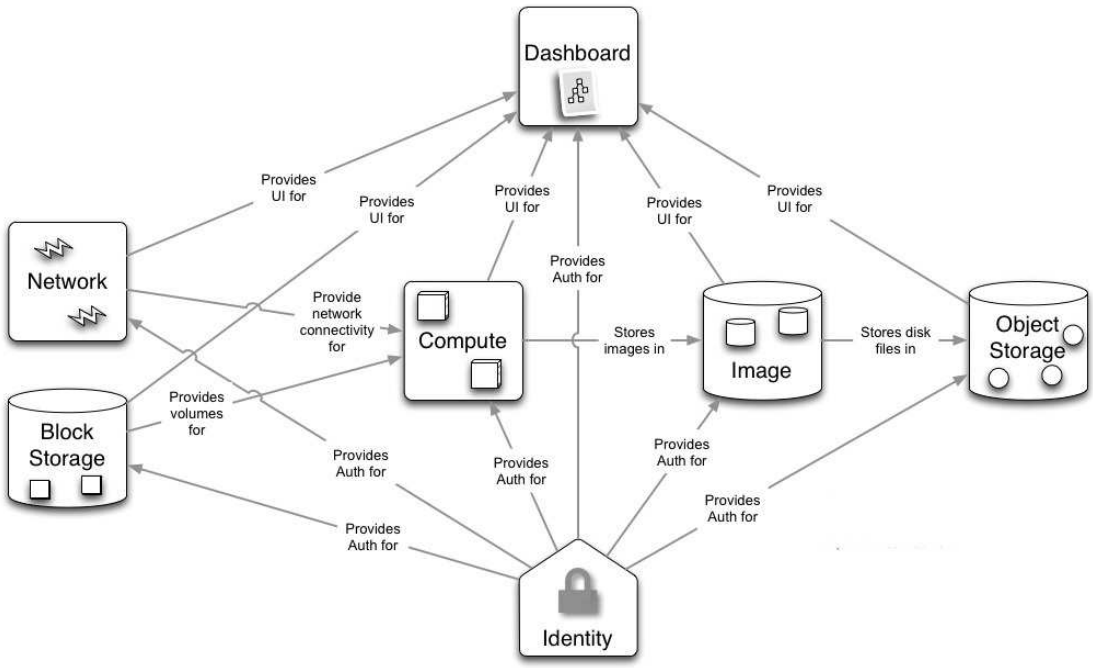


Рис. 3 Концептуальна архітектура OpenStack.

Найбільший внесок в розробку OpenStack внесли такі компанії як Rackspace, Red Hat, HP і IBM.

По мірі розвитку OpenStack і розробки нових функціональних можливостей було створено важливий сервіс, який виграє від IaaS під управлінням OpenStack – це база даних як послуга(DBaaS). Розробкою цього сервісу займається проект Trove. Для операторів мобільного зв’язку DBaaS може розглядатись як один із основних елементів сучасної архітектури, так як операторам необхідно зберігати значний об’єм даних про абонентів, послуги та ін.

В основі лежить відкрита база даних MySQL, яка забезпечує необхідні для підприємства функціональні можливості, в тому числі і мультиорендність(multi-tenancy). Функцією БД є зберігання даних, аналіз і вилучення даних для додатків. Основна задача Trove – надати користувачам OpenStack можливість легко і оперативно управляти БД. На рис.2 зображено

модель Trove.

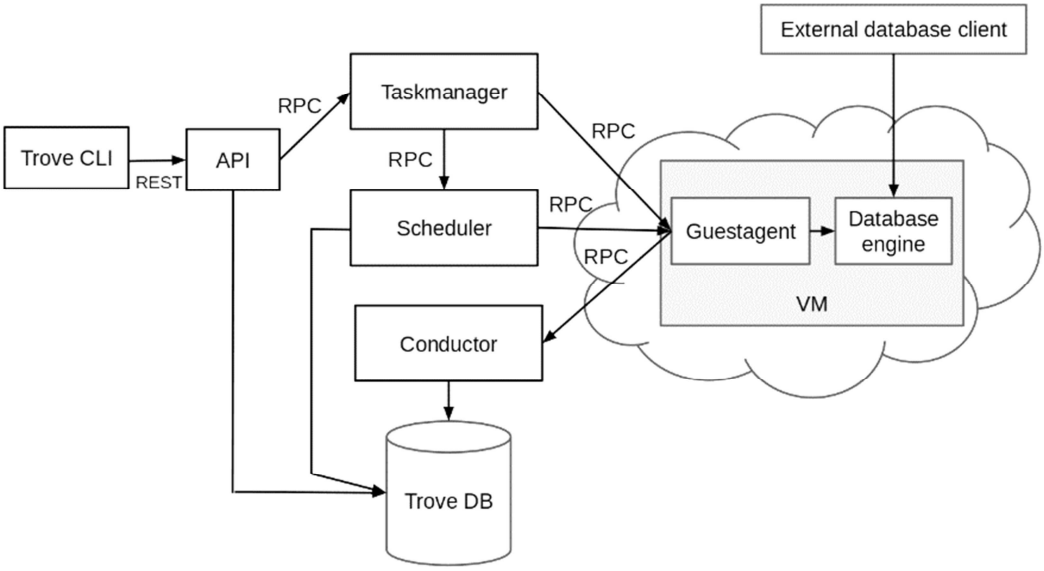


Рис. 4 Модель Trove.

На даний момент обмеженням DBaaS платформи OpenStack є те, що вона поки не підтримує одночасну роботу всіх екземплярів сервісу з одним клієнтом. Але в той же час однією з найважливіших можливостей є мультиорендність. Це означає, що один екземпляр ПЗ надає сервіси декільком клієнтам. Це означає, що крім використання цієї послуги самим оператором для переносу внутрішньої архітектури збереження даних в хмару, її можна надавати і абонентам, які цього потребують. Що може бути вигідним в фінансовому плані для компенсації витрат на підтримку хмарної інфраструктури.

Таким чином, для модернізації інфраструктури оператора мобільного зв'язку можливий її переніс у IaaS-хмару, на основі якої можна реалізувати різні сервіси як для внутрішніх цілей компанії, так і надавати «хмарні» послуги мобільним абонентам.

Література

1. Кириллов И. «Облака» в Украине: как меняется рынок. «СЕТИ И БИЗНЕС» / Игорь Кириллов. // «СЕТИ И БИЗНЕС». – 2015. – С. 42–52.
2. Кравчук С. О. , Міночкін Д. А. Застосування розподілених обчислень в телекомунікаційних системах / С. О. Кравчук, Д. А. Міночкін. // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – 2015. – №50. – С. 41–44.
3. Облако OpenStack: мифы и реальность [Електронний ресурс] // Инфосистемы Джет. – 2014. – Режим доступу до ресурсу: https://habrahabr.ru/company/jetinfosystems/blog/247087/.
4. Enterprise OpenStack and DBaaS [Електронний ресурс] // Mirantis. – 2014. – Режим доступу до ресурсу: https://www.mirantis.com/blog/enterprise-openstack-dbaas/.

УДК 621.39

ВЕРТИКАЛЬНА ПЕРЕДАЧА ОБСЛУГОВУВАННЯ В БЕЗПРОВОДОВИХ МЕРЕЖАХ

Заєць І.О. Міночкін Д. А.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: ivzaiets@gmail.com

Analysis of vertical handover in wireless network

Wireless networks are becoming a combination of more and more diverse and complicated network. General classification of vertical handoff. Thus, in this paper we analyzed the existing methods of vertical handoff.

На сьогоднішній день, неможливо уявити життя людства без доступу до мережі Інтернет. Все частіше, для цього використовуються гетерогенні безпроводові мережі, що являють собою поєднання різних безпроводових технологій. Гетерогенні мережі використовуються для того, щоб забезпечити більш широке покриття і високу пропускну здатність. Однак, це призводить до ефекту накладання, коли ієрархії різних мереж входять в зону покриття одна одної). Термінал вибирає відповідну мережу для обміну даними, опираючись на деякі параметри, такі як, наприклад, доступна пропускна здатність або потужності сигналу. Мобільний пристрій з декількома інтерфейсами може отримати доступ до більше ніж однієї мережі, в залежності від необхідної пропускної здатності. При цьому, коли мобільний пристрій змінює свою точку підключення, відбувається процес передачі обслуговування від однієї мережі до іншої. Процес передачі обслуговування між різними мережами в області накладання називають вертикальною передачею обслуговування. На сьогодні, існує велика кількість методів вертикальної передачі обслуговування, що мають різні параметри, властивості та підходи до управління мобільністю. Тому, необхідно провести аналіз існуючих методів вертикальної передачі обслуговування з метою їх подальшої класифікації.

Для ефективного аналізу необхідно визначити узагальнюючі параметри, за якими можна провести порівняння. Основні показники будь-якої системи складаються з масштабованості та витрат на передачу службової інформації, що може призвести до втрати або затримки передачі даних. Для вертикальної передачі обслуговування, необхідно визначити

базовий тип передачі обслуговування, та необхідність змін в мережевій інфраструктурі для його реалізації. Отже, загальну класифікацію можна проводити за наступними параметрами.

Процес передачі обслуговування. Робота схем управління мобільністю залежить від типу передачі обслуговування, який може бути або м'який, або жорсткий. М'яка передача обслуговування (безшовна передача обслуговування) забезпечує плавну передачу, дозволяючи терміналам спілкуватися і обмінюватися даними з декількома інтерфейсами одночасно. Зв'язок через старий інтерфейс переривається, коли рівень сигналу від відповідної точки доступу падає нижче певного порогового значення. З іншого боку, в результаті жорсткої передачі обслуговування абоненти втрачають зв'язок зі старою точкою доступу, коли рівень сигналу нижче порогового значення перед підключенням до нової.

Масштабованість. Цей параметр відноситься до здатності схеми управління мобільністю обробляти велику кількість мобільних абонентів або точок доступу. Схема масштабована, коли її продуктивність не падає зі збільшенням розміру мережі або кількості мобільних терміналів.

Витрати на передачу службової інформації. В процесі передачі обслуговування можливі втрати або затримки пакетів, що призводить до помилкової індикації перевантаження в мережі. Причиною цього є надмірність службової інформації, пов'язаної з процесом передачі обслуговування.

Зміни в мережі. Схема управління мобільністю може потребувати додаткових програмних агентів (наприклад, Home / Foreign агентів в Mobile IP) або апаратного забезпечення, яке необхідно розгорнути в існуючій мережевій інфраструктурі. Такі додаткові агенти або апаратні засоби можуть привести до проблем масштабованості та складності реалізації на існуючих мережах.

Тому, на підставі запропонованих параметрів, було проведено аналіз існуючих методів вертикальної передачі обслуговування [3]. Результати аналізу представлені в табл. 1.

Таблиця 1. Аналіз існуючих методів вертикальної передачі обслуговування.

Метод	***Тип передачі***	***Масшта-бованість***	***Додаткові витрати на службову інформації***	***Зміни в мережі***
MIPL	М'який	Так	комутація інтерфейсів	програмний агент
USHA	М’який	Так	Ретунелювання	Додатковий сервер для передачі обслуговування
SIP	М’який	Так	Реконфігурація	Ні
P-Handoff	М’який	Так	Ні	Зміна стеку протоколів
OmniCon	Жорсткий	Так	MIP затримки	Програмний агент
SIGMA	М’який	Так	Ні	Модифікація IP протоколу
mSCTP	М’який	Так	Ні	Транспортний протокол SCTP

Таким чином, в роботі проаналізовані існуючі методи вертикальної передачі обслуговування. Проведений аналіз показав, що більшість існуючих методі вертикальної передачі обслуговування задовольняють потреби масштабованості та мінімізації витрат на передачу службової інформації. Однак, для їх реалізації необхідні зміни в мережі оператора зв’язку. Тому, доцільно провести подальші дослідження існуючих методів з метою зменшення впливу їх реалізації на мережеву інфраструктуру.

Література

1. А.Д. Гришаева, В.Я. Воропаева. Выбор параметров и разработка критерия для процедуры вертикального хэндовера // Збірник наукових праць XIII науково-технічної конференції аспірантів та студентів в м. Донецьку 14-17 травня 2013 р. — Донецьк, ДонНТУ, 2013. — С. 39-41.
2. Zekri, M., Jouaber, B., and Zeghlache, D. (2012). A review on mobility management and vertical handover solutions over heteroge-neous wireless networks.Computer Communications, 35(17):2055–2068
3. J. Márquez-Barja, C. T. Calafate, J.-C. Cano, P. Manzoni, "An overview of vertical handover techniques: Algorithms, protocols and tools," Computer Communications, vol. 34, pp. 985-997, 6/1/ 2011.

УДК 621.396.1

КООПЕРАТИВНЕ РОЗНЕСЕННЯ СИГНАЛІВ В СИСТЕМІ РАДІОЗВ'ЯЗКУ

Ляшенко О. В., Кравчук С. О.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: oleksandr_lyashenko@ukr.net

Cooperative diversity of signals in the wireless system

In this article, the cooperative diversity in the wireless system as a way to wrestle multipath waves. The major idea is a sharing of multiple signals separated by a certain parameter or coordinate. It was compared of different methods of combining the output signals of the individual antennas.

Значне збільшення швидкості передачі даних і підвищення якості обслуговування користувачів (зменшення ймовірності помилки передачі інформації є однією з головних вимог в області безпроводових систем зв'язку є значне збільшення швидкості передачі даних і підвищення якості обслуговування користувачів (зменшення ймовірності помилки передачі інформації). Ця проблема особливо актуальна в мобільних безпроводових системах зв'язку, що працюють в складних умовах поширення сигналів. Загальновизнані шляхи її вирішення, пов'язані з розширенням частотної смуги або зі збільшенням випромінюваної потужності, вичерпали себе через високу вартість частотних діапазонів і вимоги біологічного захисту.

Поширення радіосигналу в міських умовах кардинально відрізняється від умов розповсюдження прямої видимості. Крім всіх перешкод і шумів з'являється безліч додаткових, небажаних ефектів. Наявність великої кількості забудов, висотних будівель, труб, структура вулиць, можливі перепади рівня земної поверхні і т. п. призводить до багаторазовому відбиттю сигналу. Навіть якщо приймальний пристрій знаходиться в стаціонарному стані, рівень прийнятого сигналу може змінюватися за рахунок віддзеркалень від рухомих транспортних засобів. В результаті на прийомну антену практично завжди приходить безліч копій сигналу (багато променів - звідси термін "багатопроменевого розповсюдження") з різними рівнями і різними затримками по часу, як це показано на рис. 1.

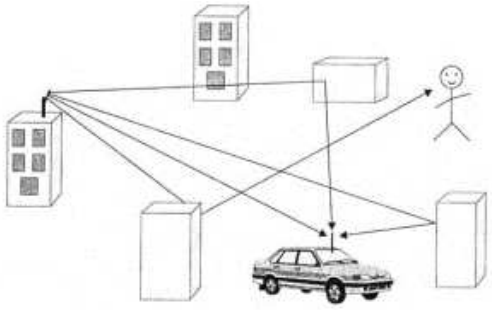


Рис. 1 Багатопроменеве розповсюдження радіосигналу.

Ідея кооперативного рознесення (англійський термін cooperative diversity, або просто diversity - рознесення) як метод боротьби з багатопроменевим розповсюдженням полягає в спільному використанні декількох сигналів, що розрізняються (рознесених) по якомусь параметру або координаті, причому рознесення повинно вибиратися таким чином, щоб ймовірність одночасних завмирань всіх використовуваних сигналів була набагато меншою, ніж якогось одного з них. Іншими словами, ефективність рознесеного прийому тим вище, чим менше корельовано завмирання в складових сигналах. Крім того, важлива технічна реалізація і простота використовуваного методу.

Найпоширенішими шляхами забезпечення кооперативного рознесення зв'язку є: просторове, частотне, часове, поляризаційне та багатопроменеве рознесення. Останнім часом для безпровідних мереж все більше використовується просторове рознесення, яке, на відміну від частотного, не вимагає розширення смуги частот. Як вказувалось вище, широко застосовується варіант рознесення N приймальних антен, розміщених на віддалях, що перевищують інтервал кореляції каналу у просторі. При цьому приймальні антени розносять на віддаль 7–10 довжин хвиль, внаслідок чого завмирання сигналу на виході окремих антен є взаємно незалежними. Варто зауважити, що найефективнішим, але і найскладнішим є метод рознесення з максимальним відношенням сигнал/шум, інші методи спрощені. Сигнали з виходу усіх приймальних антен, тобто гілок рознесення, подаються на пристрій їх сумісного оброблення та в результаті комбінування утворюють результуючий сигнал усіх гілок. Якщо на виході кожної і-тої приймальної антени амплітуда сигналу становить A_i, фаза φ_i, середньоквадратичне відхилення шуму δ_i, то оптимальним ваговим коефіцієнтом для цієї гілки є:

$$w_i = q_i e^{-j\phi i} \quad (1)$$

де $q_i = \frac{A_i}{\delta_i}$. Результуючий сигнал усіх гілок формується в такий спосіб:

$$A_s = \sum_{i=1}^{N} w_i \cdot u_i, \quad (2)$$

де $i = 1$ - вихідний сигнал *i*-ої гілки.

В результаті отримаємо результуюче відношення сигнал/шум за потужністю:

$$q_r^2 = \sum_{i=1}^{N} q_i^2. \quad (3)$$

Бачимо, що за оптимального вибору вагових коефіцієнтів забезпечується максимально можливе результуюче відношення сигнал/шум. Але така реалізація можлива за відомих значень A_i, φ_i, δ_iна виході кожної антени. При цьому сигнали окремих антен додаються когерентно після відповідного амплітудного зважування згідно з алгоритмом (2). Отже, можна отримати середнє значення відношення сигнал/шум вище порогового навіть у разі, коли в кожному з каналів воно менше від порогового. Але цей метод використовує дані про відношення сигнал/шум та фазу сигналів окремих гілок, що може вимагати додаткового пілотного каналу.

Запропоновано комбінований метод попарного (всі можливі комбінації з N по 2) обробки сигналів окремих антен та застосування до отриманих сигналів комбінування з автовибором. Ймовірність появи бітових помилок для каналу з розподілом Релея за оптимального когерентного додавання, у випадку використання N антен на приймальній стороні, визначається так:

$$P_b = \frac{1}{2} \cdot \frac{N}{(N+\frac{E_b}{N_o})^N}, \quad (4)$$

де $\frac{E_b}{N_o}$ – відношення енергії біта до спектральної густини шуму.

На табл. 1 показано залежності P_b $(\frac{E_b}{N_o})$ від кількості антен на приймальному стороні, визначені згідно зі співвідношенням (4).

Таблиця 1. залежності P_b від кількості антен на приймальній стороні

$P_b=10^{-3}$	
N	E_b/N_o,dB
N=1	28
N=2	16.4
N=3	13.4
N=4	12
N=5	11
N=100	8

Бачимо, що за збільшення гілок рознесення енергетичний виграш збільшується повільно, а складність обладнання зростає. Тому більше трьох гілок рознесення використовувати недоцільно. Варто зауважити, що за нескінченного збільшення гілок рознесення результати збігаються з даними для модуляції 2-DPSK та наявності білого гауссового шуму (AWGN). Отже, оптимальне кооперативне рознесення здатне загалом повністю усунути втрати енергетики радіоліній, зумовлені завмираннями.

Висновки. Наявність багапроменевого поширення хвиль призводить до завмирань прийнятого сигналу. Для забезпечення заданої ймовірності появи бітових помилок необхідно в сотні разів збільшувати потужність випромінювання. Розглянуто особливості рознесеного приймання, реалізованого використанням декількох антен на приймальному боці. Проведено порівняння різних методів комбінування вихідних сигналів окремих антен та дано рекомендації щодо їх застосування.

Література

1. Кравчук С.О., Міночкін Д.А., Чумак В.К. Напрямки вдосконалення технології MIMO // Зб наукових праць Військового інституту Київського національного університету ім. Тараса Шевченка. –К.: ВІКНУ, 2008. –Вип. 15.–С. 153–159
2. Zheng L., Tse D. N. C. Diversity and multiplexing: A fundamental tradeoff in multiple antenna channels // IEEE Transactions Information Theory. -2003. – Vol. 49, No 5. – P. 1073 –1096
3. Вишневский В.М., Ляхов А.И., Портной С.Л., Шахнович И.В. Широкополосные безпроводные сети передачи информации. – М.: Техносфера, 2005. – 592 с. 2. Галкин В.А. Цифровая мобильная радиосвязь: Учебн. пособие для вузов. – М.: “Горячая линия-Телеком”, 2007. – 432 с

УДК 621.396.1

СХЕМА УПРАВЛІННЯ ДОСТУПОМ ДО РАДІОКАНАЛУ ДЛЯ MESH-МЕРЕЖІ НА ОСНОВІ АЕРОПЛАТФОРМИ

Кравчук С.О.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: sakravchuk@ukr.net

Radio-channel access control scheme for mesh-network based aeroplatform

A new scheme to control access to the radio medium for mobile mesh-based network UAVs that scheme named as MAC-level aeroplatform - MAC_HAPS (Medium Access Control for HAPS). MAC_HAPS control distance, frequency of erroneous bits and determine counter attempts gear. To demonstrate the effectiveness of the scheme MAC_HAPS it was compared with the scheme MAC-level standard IEEE802.11g by numerical simulations. The simulation results showed that the delay from end to end when the scheme was less MAC_HAPS that can be explained in this case using directional antennas, and therefore better energy on the radio.

На даний час великий інтерес для побудови сучасних розподілених телекомунікаційних безпроводових мереж має створення мережних вузлів на базі аероплатформ із безпілотних літальних апаратів (БЛА) [1, 2]. Якщо раніше БЛА в основному використовувались для військових цілей, то з появою тенденції створення комерційного безповодового обладнання низької вартості COTS (Commercial Off-The-Shelf) їх застосування все більш зростає. Шляхом розміщення обладнання на аероплатформі БЛА можуть бути утворені багатоінтервальні економічно ефективні безпроводові мережі зв'язку. При цьому використовують стандартні безпроводові технології, зокрема протоколи стандарту 802.11. Однак, такі стандартні протоколи не пристосовані до роботи в мережі з рухомими вузлами, та не враховують особливості самої аероплатформи. Все це знижує ефективність застосування стандартних підходів, та породжує необхідність розробки нових протокольних схем, які врахують особливості мережних вузлів на базі аероплатформ. Тому, метою даної роботи є розробка нової схема управління доступом до радіо-середовища для mesh-мережі, що базується на БЛА.

Для мобільної mesh-мережі на базі БЛА пропонується нова схема управління доступом до радіо-середовища, що названа як схема MAC-рівня для аероплатформи – MAC_HAPS (Medium Access Control for HAPS). В даній схемі прийнято, що усі БЛА розміщуються над землею на різних висотах. Відстань між будь-якими сусідніми БЛА не перевищує межу діапазону роботи спрямованої бортової антени. Коли пакет надходить від верхнього рівня, вузол мережі потребує інформації про місце положення призначення пакету, з тим щоб направити головний пелюсток антенної системи в цьому напрямку.

Схема MAC_HAPS використовує для свого управління RTS/CTS (англ. Request To Send / Clear To Send - запит на відправку / дозвіл відправки) -

механізм CSMA/CA, який використовується в безпроводових мережах стандарту IEEE 802.11 для виключення колізій кадрів; спосіб вирішення проблем «прихованого вузла» і «незахищеного вузла».

Вузол, що бажає відправити інформацію, посилає RTS-кадр. Цільовий вузол відповідає CTS-кадром. Будь-який інший вузол, що отримав CTS-кадр, повинен утриматися від відправки інформації на заданий час (рішення Проблеми прихованого вузла). Будь-який інший вузол, що отримав RTS-кадр, але не CTS-кадр від передачі інформації утримуватися не повинен (вирішення проблеми незахищеного вузла). Кількість часу, який повинен очікувати інший вузол перед спробою доступу до ефіру, записано і в RTS-кадрі, і в CTS-кадрі.

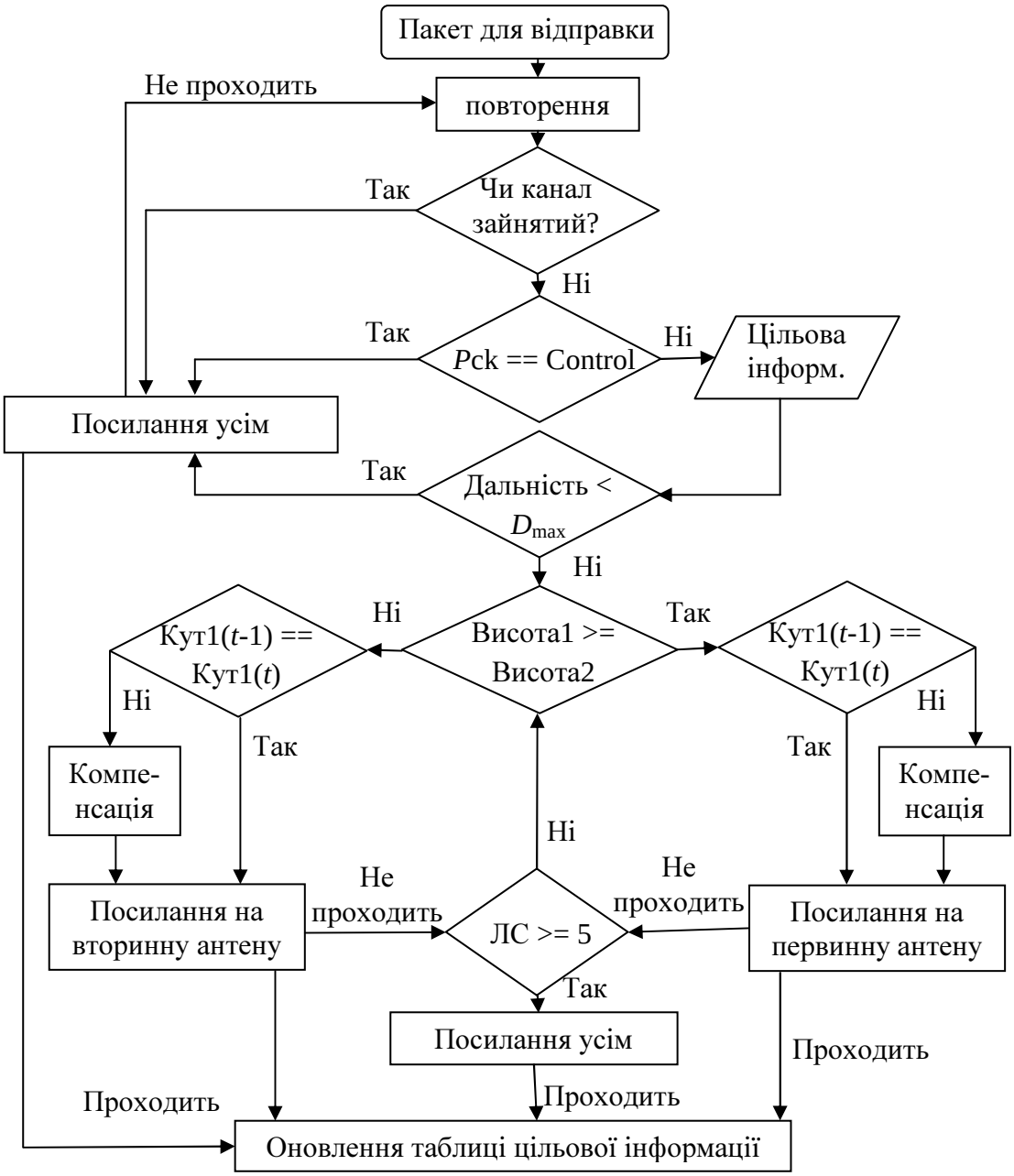


Рис. 1 Блок-схема MAC_HAPS.

Пакет управління RTS-типу буде відправлений за допомогою всенаправленої антени; вона повинна включати в себе положення літального

апарату і тривалість передачі. Отримавши це повідомлення, вузол призначення буде реагувати посилкою пакету CTS через всенаправлену антену. Кожен вузол, який приймає повідомлення CTS або RTS повинен кешувати цю інформацію і оновлювати свою таблицю маршрутизації для подальшого використання. Сам пакет даних буде передаватися з використанням спрямованої антени. Блок-схему MAC_HAPS представлено на рис. 1.

В мережі на основі MAC_HAPS-схеми кожен БЛА повинен мати чотири антени, дві з яких є спрямованими а інші - всенаправленими. Одна із спрямованих антен розташована на верхній поверхні БЛА і промаркована як первинна, друга антена розташована під фюзеляжем БЛА і маркується як вторинна. Якщо БЛА має пакет для відправки, він буде використовувати спрямовану антену, в іншому випадку для прийому пакетів від інших безпілотних літальних апаратів - всенаправлену антену. Протоколи MAC_HAPS повинні часто контролювати позиції інших безпілотних літальних апаратів і обчислювати вплив кутів Ейлера на орієнтацію спрямованої антени. Кути Ейлера визначають відносну орієнтацію між двома ортогональними системами декартових координат в 3D; описують три послідовних повороти однієї системи координат для приведення її у відповідність з іншим.

Крім того, MAC_HAPS повинен контролювати відстані, частоту появи помилкових бітів і лічильник спроб (ЛС) передач. У разі, коли активності немає протягом періоду однієї секунди, повідомлення щодо підтримки працездатності вузла надсилається за допомогою всенаправленої антени. Це повідомлення використовується для поновлення інформації про розташування БЛА. При цьому припускається, що БЛА здатний електронним способом направляти діаграму спрямованої антени в бік певного напряму. У разі, коли повітряне судно змінюватиме свою висоту зависання, діаграма спрямованості антени буде обертатися щодо своєї осі, що призводить до коливань коефіцієнта підсилення антени. Таким чином, протокол управління повинен компенсувати будь-які зміни руху БЛА.

Щоб продемонструвати ефективність схеми MAC_HAPS її було порівняно зі схемою MAC-рівня стандарту IEEE802.11g. Для моделювання використано програмний пакет OPNET, що представляє собою дискретний мережний симулятор із багатим набором детальних моделей для мереж ad-hoc і mesh. Результати моделювання продемонстрували, що затримка з кінця в кінець у випадку схеми MAC_HAPS була меншою, що можна пояснити використанням у даному випадку спрямованої антени, а отже і кращої енергетики на радіолінії.

Література

1. Srinivasan S., Latchman H. Airborne traffic surveillance systemsvideo surveillance of highway traffic // In Proc. of the ACM 2nd international workshop on Video surveillance, 2004.
2. Ильченко М.Е., Кравчук С.А. Телекоммуникационные системы на основе высотных аэроплатформ. – К.: Наукова думка, 2008. – 580 с.

УДК 621.396.1

ПОРТАТИВНА ТРОПОСФЕРНА РАДІОРЕЛЕЙНА СТАНЦІЯ ЗВ'ЯЗКУ

Кравчук С.О.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail:sakravchuk@ukr.net

Portable tropospheric radiorelay stations

The draft national portable troposphere radiorelay station of frequency range 4...5 GHz, its design and basic specifications.

Метою даної роботи є представлення проекту вітчизняної портативної радіорелейної тропосферної станції (ТРРС), основні принципи побудови якої було представлено в [1, 2].

Основними конструктивними складовими частинами станції портативної радіорелейної тропосферної є наступні (рис. 1): пристрій модемний; пристрій антенно-поворотний (ПАП); блок приймально-передавальний; блок живлення; кабель високочастотний; кабель живлення; кабель сигналізації; пристій контролю та управління дистанційний (може бути планшет) (рис. 1).

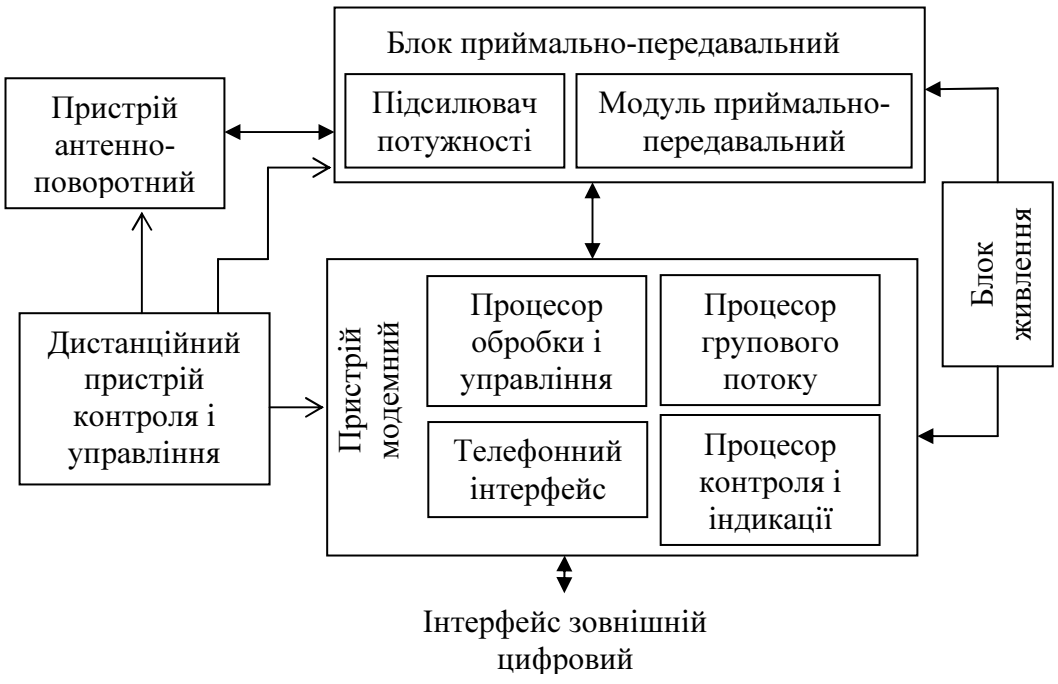


Рис. 1 Основні конструктивні складові частини ТРРС.

Обладнання ТРРС будується по блочно-модульному принципу на базі єдиних уніфікованих конструкцій, розроблених з використанням сучасної та перспективної мікроелектронної елементної бази. Устаткування ТРРС є максимально уніфікованим. Конструкція елементів виробу побудовано за модульним принципом, заміна модулів не вимагає ручної перебудови

обладнання. Можлива компоновка ТРРС з ручним управлінням ПАП: звичайна; з рознесенням антен (MIMO-режим); з двома незалежними виходами; з рознесенням по діапазонам. Зовнішній вигляд портативної ТРРС представлено на рис. 2.

До складу антенно-поворотного пристрою входять: тринога, антена і поворотний пристрій. Функціональний склад блоку приймально-передавального: підвищувальний конвертер частоти; підсилювач потужності з можливістю управління коефіцієнтом підсилення; дуплексерні фільтри на передачу та прийом; малошумливий понижуючий конвертер частоти; пристрій вбудованого автоматичного контролю виробу; елементи вторинного електроживлення вузлів виробу; перехід на антенний хвилевід круглого перерізу. До складу модемного пристрою входять плати: блоку обробки та управління; процесора групового потоку і контролю та індикації; інтерфейсу телефонного; блоку вторинних джерел живлення.

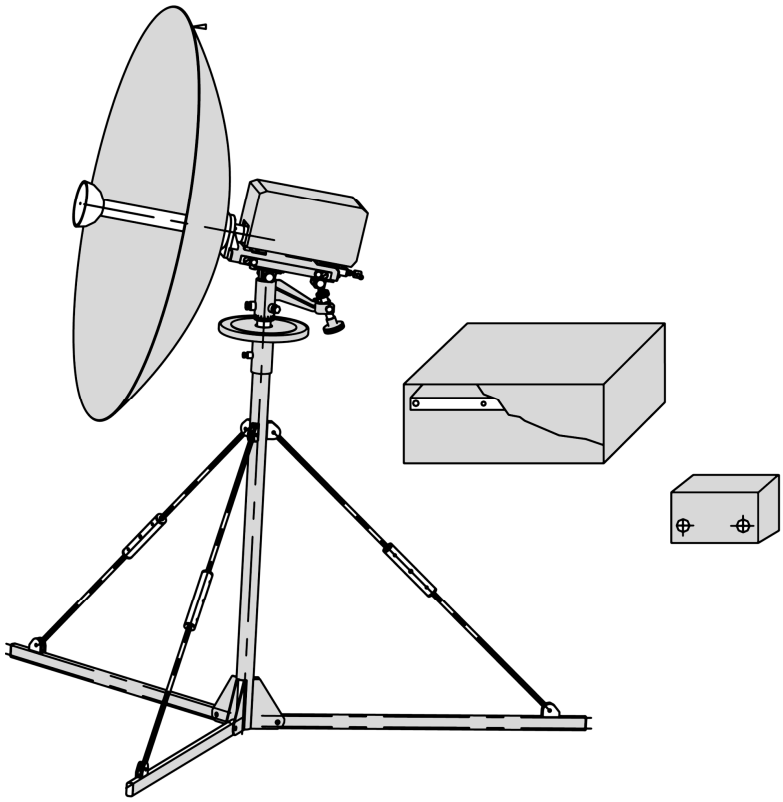


Рис. 2 Зовнішній вигляд портативної ТРРС.

Розроблена ТРРС повинна мати наступні основні технічні характеристики: швидкість прийомо-передачі цифрового інформаційного потоку до 8048 кбіт/с; зв'язок в мережі Ethernet 100 BASE-TX, рознім - RJ45-IP67 і наявність портів з можливістю інкапсуляції зовнішнього потоку конвертора E1 (G.703) в Ethernet; діапазон робочих частот виробу - 4,4...5,0 ГГц; вихідна потужність передавача на антенному фланці повинна бути приблизно 200 Вт; можливість автоматичного дискретного (з кроком 1 дБ) регулювання вихідної потужності - не менш 30 дБ; наявність вбудованої системи функціонального контролю без випромінювання в ефір; величина

побічних складових випромінювання ТРРС щодо рівня гармонічних, інтермодуляційних складових та інших видів випромінювань повинна відповідати вимогам діючих стандартів.

Система управління і контролю станції будується за розподіленою багатопроцесорною архітектурою з централізованим управлінням, до складу системи входять процесор управління станції, процесор контролю та індикації, процесор управління синтезаторами частоти модему, які фізично входять до складу модему, а також управляючі пристрої, які входять до складу других блоків станції.

Процесор управління тропосферної станції виконує функції центрального процесора системи. Для зв'язку з зовнішніми пристроями процесор використовує чотири інтерфейси: високошвидкісний послідовний інтерфейс SPI для обміну з процесором групового потоку; інтерфейс RS-485 для управління і контролю периферійними процесорами, які знаходяться в приймально-передавальному блоці станції, а також з процесором управління синтезаторами частоти модему; інтерфейс RS-232C для формування каналу службової інформації і управління мережею тропосферних станцій; послідовний двонаправлений інтерфейс для обміну інформацією з процесором контролю та індикації.

Управління і контроль периферійних процесорів здійснюється в режимі передачі пакетів, які складаються з адреси джерела інформації, адреси отримувача інформації і поля даних. Периферійні процесори, що здійснюють контроль і управління приймально-передавальним блоком станції розташовуються безпосередньо в ньому.

Конструктивно процесор контролю і індикації виконаний у вигляді окремої плати, яка встановлена в корпусі модему і з'єднується роз'ємами з блоком обробки і управління, з платою світлодіодів, з клавіатурою, з індикатором і з джерелом живлення.

Література

1. Кравчук С.О. Принципи створення портативних тропосферних радіорелейних станцій // Матер. 9-ї міжнар. наук.-техн. конф. "Проблеми телекомунікацій", 21–25 квітня, 2015 р. – К.: НТУУ «КПІ», 2015. – С. 254–256.
2. Проектирование модема современных тропосферних радиорелейных станций / А.Г. Войтенко, Н.Н. Кайденко, С.А. Кравчук, Т.Н. Нарытник // Матер. 23-й Международной Крымской конф. «СВЧ-техника и телекоммуникационные технологии» (КрыМиКо'2013). Севастополь, 8–13 сентября 2013 г. – Севастополь: Вебер, 2013. – С. 326–327.

УДК 621.396.1

МОДЕМНИЙ ПРИСТРІЙ ДЛЯ ТРОПОСФЕРНОЇ РАДІОРЕЛЕЙНОЇ СТАНЦІЇ

Кайденко М.М., Кайденко В.М., Кравчук С.О., Роскошний Д.В.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail:sakravchuk@ukr.net

Modem device for tropospheric radiorelay stations

Developed modem device for a portable troposphere radiorelay station. The modem provides control station channel-forming and interface with external networks.

На даний час підвищення інтересу до розробки та модернізації тропосферних радіорелейних станцій (ТРРС) потребує створення високоефективного спеціального каналоутворюючого обладнання, основою якого є модемний пристрій [1-3]. Метою даної роботи є розробка модемного пристрою для портативної ТРРС «Чайка» для забезпечення підтримки необхідної завадостійкості в умовах багатопроменевих завмирань та конкурентоздатності зазначеної ТРРС по відношенню до інших систем безпроводового доступу.

Пристрій модемний, далі модем, призначений для використання в складі тропосферної станції та виконання наступних функцій:

- об’єднання в груповий цифровий потік даних сигналів передачі даних Ethernet – до 8048кбіт/с, службової інформації управління мережею тропосферних станцій – до 64 кбіт/с (опція), каналу сигналізації – до 64 кбіт/с та до 4 голосових каналів по 32 кбіт/с (опція);
- перетворення цифрового потоку даних в фазоманіпульований сигнал ФМ4 проміжної частоти передавача з центральною частотою 400 МГц;
- перетворення фазоманіпульованого сигналу ФМ4 проміжної частоти приймача з центральною частотою 180 МГц в цифровий потік даних;
- розділення цифрового групового потоку даних на сигнали передачі даних Ethernet – до 2048кбіт/с, службової інформації управління мережею тропосферних станцій – до 64 кбіт/с (опція), каналу сигналізації – до 64 кбіт/с та до 4 голосових каналів по 32 кбіт/с (опція);
- формування сітки частот приймача та передавача тропосферної станції;
- прямої корекції помилок в каналі з використанням згорткового кодування (опція) та кодування кодом Ріда-Соломона (204,188,8);
- безперервного неруйнуючого контролю помилок на рівні декодера Ріда-Соломона з індикацією коефіцієнта помилок;
- формування в груповому цифровому потоці каналу управління мережею тропосферних станцій (опція);
- управління режимами роботи тропосферної станції з пульта управління або зовнішнього терміналу: призначення робочих частот приймача та

передавача, управління атенюаторами, автоматичне тестування працездатності тропосферної станції;
- контролю стану тропосферної станції та відображення інформації на індикаторі, або на зовнішньому терміналі.

Основні технічні вимоги до модему:

Інформаційний інтерфейс модему	Ethernet 10/100 BASE-Tx
Центральна частота ПЧ модулятора, МГц	400
Потужність сигналу на виході ПЧ модулятора, дБм	-20…. - 0
Кількість під несучих частот в робочій смузі	1…3
Ширина смуги частот тракту ПЧ, МГц	120
Потужність сигналу на вході приймача, дБм	0….-40
Модуляція	ФМ4
Завадостійке кодування:	
Параметри згорткового коду	К=7(171,133)
Швидкість згорткового коду	1/2, 2/3, 3/4, 7/8
Смуга частот окремих піднесучих, не більше МГц	1,25/2,5/5 1,75/3,5/7
Діапазон автоматичної підстройки частоти (ФАПЧ), мінімум, кГц	250
КСХн по входу та виходу в смузі частот (fo±3,5МГц),од., не більш	1,2
Нерівномірність АЧХ в смузі частот піднесучої (*f*o ±3,5 МГц), дБ, не більш як	0,3
Відносна нестабільність частоти по виходу ПЧ модулятора	$3 \cdot 10^{-6}$
Протокол та інтерфейс передачі даних	IP, Ethernet
Протокол та інтерфейс керування	SNMP, Ethernet
Роз’єм передачі даних	RJ 45
Роз’єм керування	RJ 45
Роз’єм ПЧ	тип *N*
Напруга живлення, В	-48
Споживана потужність, Вт, не більше	30,0

Конструктивно модем виконується у вигляді окремого блоку, до складу якого входять: плата блоку обробки та управління; плата процесора групового потоку; плата процесора контролю та індикації; плата інтерфейсу телефонного; плата світлодіодів; клавіатура; рідкокристалічний індикатор; блок вторинних джерел живлення.

Узагальнена структурна схема модему представлена на рис. 1.

Сигнали від зовнішнього обладнання поступають на вхід процесора групового потоку. Обмін з обладнанням Ethernet здійснюється на швидкості 10/100 Мбіт/с в режимі напівдуплексу. Швидкість даних Ethernet в груповому потоці складає до 2048 кбіт/с (в залежності від режиму роботи) в одному напрямку передачі. Сигнали голосового зв’язку (при використанні такої опції) можуть поступати як від гарнітури, що підключається безпосередньо до модему, так і від виносного пристрою, якій може бути віддалений на

відстань до 100 м. В процесорі групового потоку з аналогових голосових сигналів формується цифровий сигнал в АДІКМ 32 кбіт/с. Додатково до групового цифрового потоку вводиться канал управління мережею тропосферних станцій 64 кбіт/с (при використанні такої опції) та канал сигналізації до 64 кбіт/с, які формуються процесором управління тропосферної станції, а також канал синхронізації, необхідний для правильної роботи обладнання. Максимальна сумарна швидкість в груповому потоці складатиме до 2,336 Мбіт/с. Як опція, в модемі може бути передбачений режим ретрансляції, при якому на іншу тропосферну станцію, що встановлюється в безпосередній близькості, по з'єднувальним кабелям передається груповий потік.

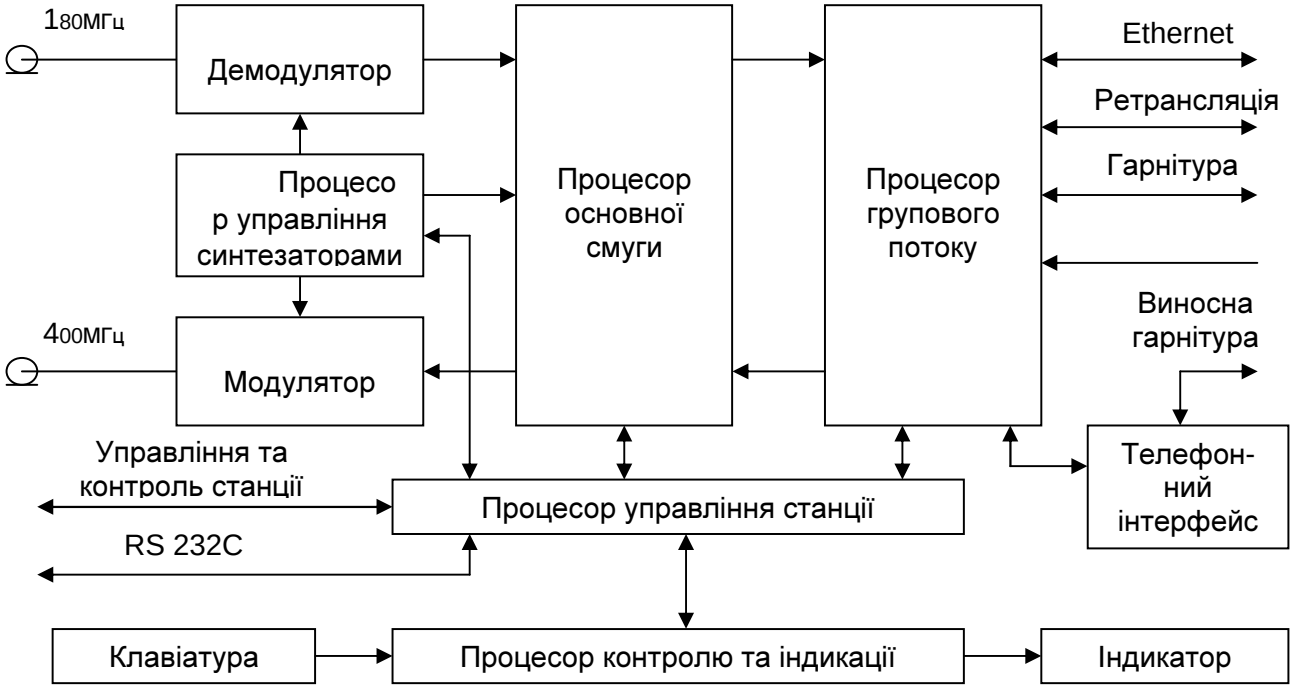


Рис. 1 Узагальнена структурна схема модему.

Сформований груповий потік поступає в процесор основної смуги частот, де здійснюється скремблювання, кодування завадостійкими кодами з прямою корекцією помилок (код Ріда-Соломона та, як опція, згортковий код), і розділення на два потоки. Кожен потік фільтрується передмодуляційним фільтром, після чого вони подаються на цифро-аналогові перетворювачі, а потім на квадратурний модулятор, де здійснюється формування фазоманіпульованого сигналу проміжної частоти. Сигнал проміжної частоти (ПЧ) після підсилення та фільтрації подається на вихідний роз'єм модему і далі, по кабелю міжблочного з'єднання, на вхід передавача приймально-передавального блоку тропосферної станції.

Сигнал проміжної частоти по кабелю міжблочного з'єднання подається з виходу тракту ПЧ приймача приймально-передавального блоку тропосферної станції на вхід демодулятора модему. В демодуляторі сигнал фільтрується, нормується по рівню схемою АРП (автоматичне регулювання

підсилення), розкладається на дві квадратурні складові з нульовою несучою частотою. Квадратурні складові фільтруються, підсилюються та оцифровуються с частотою чотири відліки на символ.

Цифрові сигнали квадратурних каналів подаються на процесор основної смуги частот, в якому здійснюється демодуляція фазоманіпульованого сигналу, тактова і кадрова синхронізація прийнятого потоку даних, дескремблювання, виправлення помилок декодером Ріда-Соломона (та у випадку використання опції зі згортковим кодуванням – декодером Вітербі) і передача даних до процесора групового потоку. В процесорі основної смуги здійснюється підрахунок помилок в каналі для подальшого обчислення коефіцієнту помилок в процесорі групового потоку.

Управління тропосферною станцією здійснюється процесором управління. Управління може бути здійснене як з клавіатури, так і з зовнішнього керуючого пристрою (ноутбук, комп'ютер, планшет). Для обслуговування клавіатури та індикатора використовується процесор контролю та індикації.

Конструктивно модем виконується в корпусі 19" 2U, який встановлюється до стійки і має габаритні розміри 483х380х88. На задній панелі модему розміщуються органи приєднання модему до приймально-передавального блоку тропосферної станції. На передній панелі модему розміщуються органи приєднання модему до зовнішнього обладнання та пристроїв, а також органи управління та контролю.

Література

1. Ільченко М.Ю., Кравчук С.О. Сучасні телекомунікаційні системи. – К.: Наукова думка, 2008. – 328 с.
2. Кравчук С.О. Принципи створення портативних тропосферних радіорелейних станцій // Матер. 9-ї міжнар. наук.-техн. конф. "Проблеми телекомунікацій", 21–25 квітня, 2015 р. – К.: НТУУ «КПІ», 2015. – С. 254–256.
3. Проектирование модема современных тропосферних радиорелейных станций / А.Г. Войтенко, Н.Н. Кайденко, С.А. Кравчук, Т.Н. Нарытник // Матер. 23-й Международной Крымской конф. «СВЧ-техника и телекоммуникационные технологии» (КрыМиКо'2013). Севастополь, 8–13 сентября 2013 г. – Севастополь: Вебер, 2013. – С. 326–327.

УДК 621.396

КАНАЛЬНА ОЦІНКА ТА АДАПТИВНА МОДУЛЯЦІЯ В СИСТЕМАХ КОГНІТИВНОГО РАДІО

Діденко І.В., Кравчук С.О.

Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: mr.untracable@gmail.com

Channel Estimation and Adaptive modulation in Cognitive Radio Systems

Channel-adaptive transmission schemes find applications in cognitive radios, which are able to measure, feed back, and adapt to, the fading channel state.

Стрімкий розвиток безпроводових телекомунікаційних систем призвів до того,що практично весь частотний діапазон до теперішнього часу розподілений і ліцензований. Однак,як показали дослідження ,спектр як дорогоцінний природний ресурс, використовується не досить ефективно. Істотно підвищити ефективність використання спектра дозволяє механізм динамічного керування спектром, відповідно до якого вторинним користувачам (не закріпленим за даним частотним діапазоном) надається можливість використовувати діапазони первинних користувачів (закріплених за даним діапазоном) на час, поки цей діапазон не використовується первинним користувачем. Цей механізм реалізований в когнітивному радіо. Системи когнітивного радіо мають здатність отримувати інформацію про своє радіочастотне середовище і адаптуватися,а саме коригувати параметри передачі для оптимальної роботи. Саме тому дослідження цих систем є досить актуальною та перспективною.

Частина роботи полягає у виборі найкращого типу модуляції, тому використовується схема зі змінним швидкістю, потужністю та адаптивною M-QAM модуляцією. Модель представляє собою канал типу точка-точка з антенами на обох кінцях з Релеївським завмиранням. Роботу схеми можна поділити на 2 етапи:тестування та передачі даних. Під час етапу тестування приймач оцінює канал і передає оцінку назад в передавач(по каналу зворотного зв’язку). Під час етапу передачі даних передавач посилає повідомлення, адаптуючи розмір M-QAM сузір’я.

Основне завдання,яке необхідно вирішити під час етапу тестування– знайти оптимальну лінійну оціночну функцію MMSE для того,щоб вирішити відповідну задачу оптимізації. Після цього розрахункове значення подається назад до передавача та починається етап передачі даних.

Із-за простоти реалізації буде використовуватися набір квадратних сузір'їв. Приклад 64-QAM сузір'я показано на Рис.1.

Основна задача етапу полягає в знаходженні коефіцієнт бітових помилок (BER) при використанні M-QAM,тому необхідно представити

сузір'я як поєднання двох $\sqrt{M}$-PAM сузір'їв, які складаються з синфазної та квадратурної компонент і представлені на Рис.2.

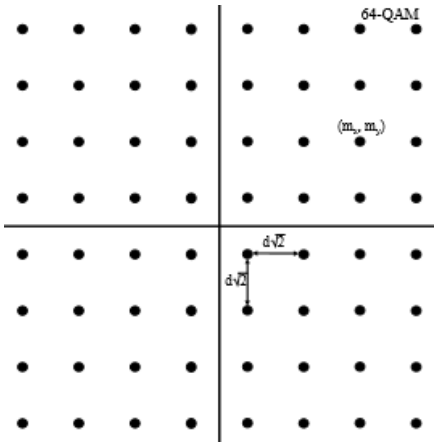


Рис. 1 Приклад 64-QAM сузір'я.

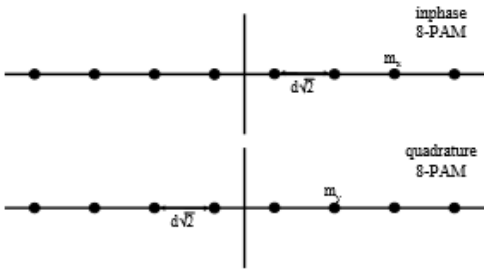


Рис. 2 Синфазне та квадратурне 8-PAM сузір'я.

Якщо немає помилки оцінки каналу, то ймовірність правильного виявлення сигнальної точки являє собою результат правильних ймовірностей виявлення в кожній із компонент відповідних $\sqrt{M}$-PAMs. Але з помилкою оцінки каналу,ймовірність правильного виявлення буде більшою ,ніж цей результат. Згідно з [1] BER може бути знайдений усередненням сигнальних точок $BER = \frac{1}{M}\sum_i \sum_j (P_{i|j} + P_{j|i})$. Для того, щоб знайти область рішень, коли існує помилка оцінки каналу в системі, використовується правило максимальної правдоподібності. Завдяки розрахункам можна виділити, що схема живлення не адаптивна, але M-QAM модуляція адаптивна, де інформація про стан каналу (CSI) використовується для адаптації розміру модуляційного сузір'я, а не потужність передачі. Вирішуючи відповідну задачу оптимізації виявляється, що тестовий сигнал, максимізує ефективне значення сигнал шум (SNR), а також, будь-який тестовий сигнал, який має одиничну енергію вважається оптимальним.

Згідно з [2] швидкість являється зростаючою функцією T_d , а тому спадаючою функцією T_t. Встановлення мінімального значення T_t що в нашому випадку дорівнює 1, являється оптимальним. Це може здатися нелогічним на перший погляд, але довший етап тестування призведе до більш точної оцінки каналу,а тому,більш досяжної швидкості передачі під час етапу передачі даних.

При використанні експериментальних формул,зробивши аналіз схеми при заданому рівні BER=10^{-2} врахувавши біти, що були помилково декодовано отримаємо залежність середнього значення BER від рівня SNR. Проаналізувавши Рис.3 можна побачити, що практичний результат BER перевищує цільове значення не в значній мірі. Також порівняємо бітрейт передачі даних схеми та теоретично можливим із заданим значенням BER за

допомогою Рис.4, де можна побачити, що схема для даного значення SNR, працює з різницею в 1 біт від теоретично можливого значення.

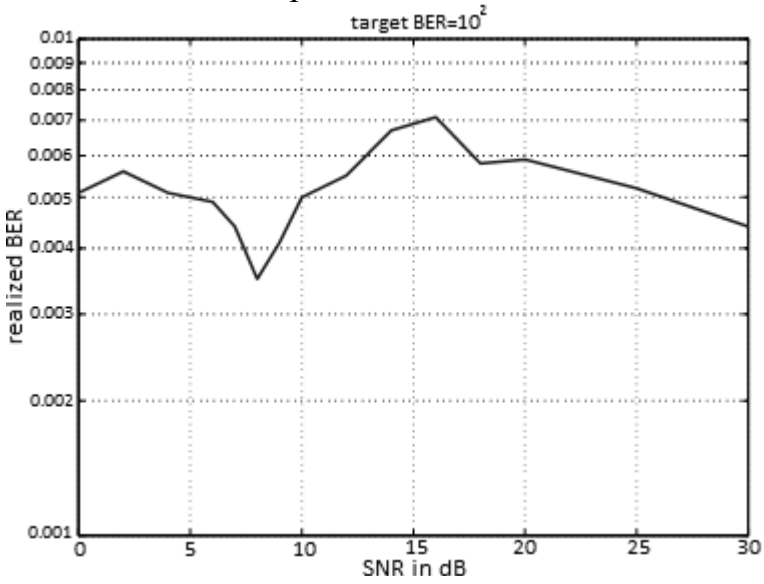


Рис. 3. Практична реалізація значення BER при заданій цілі BER=10^{-2}.

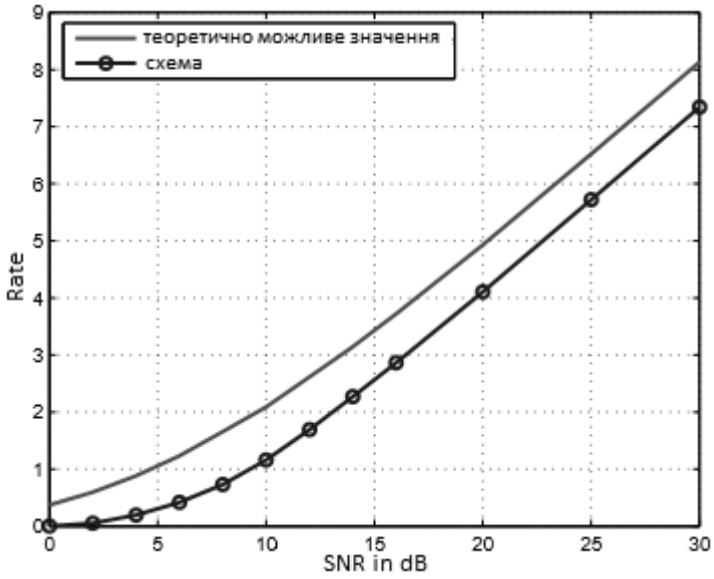


Рис. 4. Отриманий бітрейт при BER=10^{-2} в порівняні з теоретично можливим.

Досліджено та проаналізовано принцип оцінки каналу з використанням адаптивної M-QAM модуляції, а також алгоритм, який дозволяє когнітивному радіо обирати оптимальний розмір M-QAM сузір'я для даного стану каналу. Наведені результати показують гарну продуктивність і дуже близькі к теоретично можливій границі.

Література

1. Channel Estimation and Adaptive M-QAM in Cognitive Radio Links / A. Soysal, S. Ulukus and C. Clancy. // IEEE Communications, 2008.
2. How much training is needed in multipleantenna wireless links? / B. Hassibi and B. M. Hochwald. // IEEE Transactions on Information Theory, 2003.

УДК 004.7

АНАЛІЗ ПРОЦЕСУ ВПРОВАДЖЕННЯ ХМАРНИХ ТЕХНОЛОГІЙ У СВІТІ

Рабченюк С.І., Прус Р.Б.
Київський національний університет імені Тараса Шевченка, м. Київ
E-mail: komawka_875@mail.ru

Analysis of cloud technology implementation in the world

Analysis of cloud technology development in different states of the world is conducted. The main ways of novel information and communication technology development are defined. The model of cloud protection, which contains specific recommendations related to various security functions and combines best practices of asset protection while using cloud services, is proposed. The governmental measures of particular countries conducted to improve the quality of service and improve security are described.

Актуальність. В ході швидкого розвитку інформаційних технологій певні сектори державних та приватних організації переходять на хмарні обчислення. У сучасному житті додатки великих постачальників послуг передаються у хмарні сховища і працюють в декількох великих центрах обробки даних. Громадські дані по поглинанню хмарних обчислень показують, що протягом декількох наступних років близько 80% організацій залежатимуть від хмарних обчислень. Подальшому розвитку і шляхам побудови нової інфраструктури різних країн, новим технологічним рішенням реалізації IT систем, присвячуються сучасні науково-практичні конференції, ведуться дослідження та публікуються огляди. Хмарні технології дозволяють створити потужну інформаційно-телекомунікаційну систему з новою архітектурою та можливостями.

Мета доповіді – проведення аналізу рівня впровадження хмарних технологій, систем та сервісів інформаційної безпеки у різних країнах світу; пропозиція розробки і застосування деяких рекомендацій щодо роботи над стратегією розвитку захищених хмарних мереж.

Міжнародне товариство провадить активні реформи в законодавчій базі на основі розробки та впровадження стандартів, технічних вимог, правових актів, тим самим сприяючи розвитку новітніх технологій у сфері інформатизації міжнародного суспільства.

Державні органи можуть бути ключовими гравцями в області хмарних обчислень, адже вони пропонують масштабованість, еластичність, високу продуктивність, стійкість до відмов і безпеку, а в той же час вона може включити й спростити взаємодію громадян з урядом за рахунок зниження часу обробки інформації, зниження вартості державних послуг та підвищення безпеки даних громадян.

У ході аналізу нормативно-правової діяльності країн, які становлять 80% світового ринку впровадження інформаційно-комунікаційних технологій, було з’ясовано, що значна частина діяльності міжнародних організацій стрімко

рухається у напрямку створення законодавчого поля сприятливого для використання хмарних технологій. Серед таких держав високу позицію посідає Японія, у на дванадцяту виходить Польща, на чотирнадцятому місці — Росія. Дослідження проводилося за сімома критеріями, що характеризують направленість законодавства на продуктивний розвиток хмарних технологій. До таких критеріїв належать: наявність положень щодо конфіденційність даних, кіберзлочинність, безпека, підтримка впроваджених бізнес-стандартів і створення й функціонування законодавства на світовому рівні.

У законодавстві України визначення хмарних обчислень узагалі відсутнє, однак у затвердженій розпорядженням Кабінету Міністрів Україна від 15 травня 2013 р. «Стратегії розвитку інформаційного суспільства в Україні» використовується поняття хмарних технологій, а саме в пункті, що передбачає формування сучасної інформаційної інфраструктури.

На підставі попереднього аналізу стану імплементації та розширення використання хмарних технологій у країнах Європи, модель Plan-Do-Check-Act (PDCA) була ідентифікована як підходяща для безперервного процесу моделювання системи менеджменту інформаційної безпеки при використанні хмарних технологій. Використання циклу PDCA підводить до визначення основи для створення захищених хмарних мереж. Ця модель застосовується у сфері інформаційної безпеки, оскільки чітко ідентифікує окремі етапи процесу і включає в себе поняття про оцінку (Check) і налаштування/оновлення (Act), що дуже важливо з точки зору усіх мережевих та інформаційних аспектів безпеки.

Модель PDCA включає наступні етапи:

1. **Plan**: Цей етап зосереджений на налаштуванні політик та їх узгодженні із стратегією реалізації управління для досягнення цілей безпеки. На етапі планування першочерговим завданням є аналіз ризиків – ідентифікація та оцінка активів, що планується розмістити у хмарі; визначення аспектів інформаційної безпеки актуальних для цих активів (захист конфіденційності, цілісності, доступності); оцінка рівня завданої шкоди у разі реалізації загроз та їх ймовірностей. Вибір архітектури (приватна, публічна, гібридна чи громадська) та моделі надання послуг (IaaS, PaaS, SaaS) також є необхідною частиною даного етапу, як і розробка вимог безпеки та конфіденційності. Наприклад, у урядом Греції розроблено мінімальні вимоги до провайдерів хмарних технологій на основі національного законодавства та вимог безпеки у галузі інформаційно-комунікаційних технологій (ІКТ), а у Об’єднаному Королівстві розроблено 14 принципів безпеки хмарних технологій, яким повинні слідувати постачальники.

2. **Do**: Цей етап включає в себе реалізацію рішень, прийнятих на попередньому етапі, причому головною метою є дотримання усіх визначених вимог безпеки. Підлягають розгляду питання передачі інформації за межі країни. Цей етап включає також акредитацію і сертифікацію та розробку угоди про надання послуг з метою контролю якості. У Іспанії, приміром, чітко визначені суб’єкти – клієнт і провайдер, що дозволяє розділити їх ролі; а самооцінка якості рішення використовується для прогнозування результатів їх впровадження.

3. **Check**: Ця фаза орієнтована на розгляд та оцінку роботи (ефективності та

результативності) системи на основі даних моніторингу (перевірка журналів, трафіку, веб-додатків, обладнання). Наприклад, у Іспанії проводять плановий аудит кожні два роки групи із внутрішніх та зовнішніх аудиторів, а також позапланові аудити для підтвердження акредитації та оцінки якості системи безпеки. У Об'єднаному Королівстві такі перевірки проводять щорічно офіційно уповноважені консультанти.

4. **Act**: Цей етап включає в себе виправлення недоліків або прогалин, виявлених на етапі перевірки – урегулювання конфлікту між клієнтом та провайдером у разі порушення угоди, оновлення системи шифрування, переакредитація, анулювання угоди із поверненням активів клієнту або їх знищенням.

Висновки. Державні органи можуть бути ключовим гравцем в області хмарних технологій, які пропонують масштабованість, еластичність, високу продуктивність, відмовостійкість і безпеку, а також ефективність витрат. У той же час вони можуть спростити громадянам взаємодію з урядом за рахунок зниження часу обробки інформації, знизити вартість послуг та підвищити безпеку даних громадян. Державним органам, у тому числі міністерствам, урядовим установам і державним адміністраціям хмарні технології пропонують великий потенціал для управління безпекою і стійкістю в традиційних середовищах ІКТ та зміцнення своєї національної стратегії розвитку хмарних технологій.

Запропоновані рішення для захисту хмарних технологій структуровані згідно широко використовуваної моделі Plan-Do-Check-Act. Представлена система розроблена на основі всебічного дослідження, яке включає вивчення сучасних практик та досвіду впровадження урядових хмарних технологій. Аналіз показав, що різні країни використовують різні практики реєстрації доказів, інструменти моніторингу, розв'язання випадків порушення угоди про надання послуг, процедури акредитації. Розроблено різні політики для управління інцидентами. У цілому, дана модель захисту хмарних технологій повинна стати одним із основних інструментів при плануванні міграції активів у хмару та при оцінці ефективності механізмів і процедур безпеки.

Література

1. 2013 BSAGlobal Cloud Computing Scorecard [Електронний ресурс]. — Режим доступу: http://cloudscorecard.bsa.org/2013/assets/PDFs/BSA_GlobalCloudScorecard2013.pdf.
2. Безопасность в облаке / Cisco [Електронний ресурс]. – Режим доступу: http://www.cisco.com/ web/UA/about/news/2011/11152011b.html.
3. Kroes Neelie. Towards a EuropeanCloudComputingStrategy / NeelieKroes [Electronicresource]. — Modeofaccess: http://europa.eu/rapid/pressReleasesAction.do?referen ce=SPEECH/11/50.
4. European Union Agency for Network and Information Security Science and Technology Park of Crete (ITE) Vassilika Vouton, 700 13, Heraklion, Greece.

УДК 004.621.3

ВИКОРИСТАННЯ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ У ПРОЦЕСІ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Алєксєєва К.І., Толюпа С.В.

Київський національний університет іме. Тараса Шевченка, м. Київ, Україна

E-mail: Karinaalekseeva@ukr.net

Analysis of computer incidents in modern information and communication systems is conducted. The main aspects and elements of information security incident management are examined. Based on a detailed analysis of incident monitoring process index performance of incident management are defined. In order to improve efficiency of incident management implementing of intellectual technology is proposed. The algorithm of intellectual system of decision-making process to improve security by optimal incident management is described.

Система управління інцидентами інформаційної безпеки є базовою частиною загальної системи управління інформаційною безпекою (СУІБ) і дозволяє виявляти, враховувати, реагувати й аналізувати події та інциденти інформаційної безпеки. Без реалізації цих процесів неможливо забезпечити рівень захищеності, що адекватний сучасним стандартам і галузевим нормам.

Управління комп'ютерними інцидентами – процес або набір процесів, на вхід яких подаються дані, отримані у результаті збору і протоколювання даних про події, що зачіпають інформаційні системи, а на виході цих процесів одержують інформацію про причини інциденту, що відбувся, про збиток, нанесений організації, і заходах, які необхідно прийняти для того, щоб інцидент не повторився. Управління комп'ютерними інцидентами спрямовано на вдосконалення системи забезпечення безпеки організації.

Реагування на інцидент - сукупність дій, спрямованих на виявлення комп'ютерної інформації, що має відношення до інциденту, і збереження її цілісності та юридичної значущості, а також на збір інших відомостей, що мають відношення до інциденту.

В останні роки істотно підвищився інтерес до дослідження, розробки й впровадження прикладних інтелектуальних систем управління. Аналіз існуючих систем управління сучасними інформаційними мережами показав, що їх рівень не відповідає повною мірою сучасним вимогам до управління мережами нового покоління, не дає змоги отримувати інформацію потрібної якості для оперативного прийняття обґрунтованих рішень щодо управління об’єктами, обміну інформацією між суб’єктами системи управління, а також не дає можливості оперативно управляти ситуаціями на мережах в автоматизованому режимі [1].

Інциденти інформаційної безпеки (ІБ) є окремим підкласом кризових і надзвичайних ситуацій, що можуть відбутися в інфо-соціо-технічній інфраструктурі та інфокомунікаційних мережах, впливаючи на стан інформаційних ресурсів і безпеки.

Основна задача управління інцидентами – якомога швидше відновити нормальну роботу служб і звести до мінімуму негативний вплив інциденту на роботу організації для підтримки якості і доступності служб на максимально

можливому рівні [2].

Специфічні питання управління інцидентами інформаційної безпеки розглядаються у наступних документах: ISO/IEC 27001:2005 Information security management system Requirements; ISO/IEC TR 18044 Information security incident management; CMU/SEI-2004-TR-015 Defining incident management processes for CISRT та ін. [3].

З кожним днем стає все складніше зберегти монополію на інформацію. Зловмисник завжди має перевагу, тому для організації дуже важливо мати змогу вдало налагодити СУІБ задля якнайшвидшого виявлення та найскорішого реагування на інциденти будь-якого роду, аби мінімізувати витрати та ліквідувати негативні наслідки. Матимемо на увазі:

- Аналіз загроз безпеки є важливою та невід'ємною складовою побудови та супроводження ІТ систем.
- Побудова моделі загроз необхідна, так як різні види інформації потрібно захищати по-різному і від різних типів загроз.
- Модель безпеки, ефективна 5-10 років тому, більше не може вважатися прийнятною для вирішення сучасних задач, оскільки на зміну відносно необразливому хуліганству в мережі Інтернет прийшла організована кіберзлочинність.

Моніторинг ІБ — один з найважливіших процесів інформаційної безпеки в організації. Програма моніторингу налаштована на миттєве реагування на будь-які відхилення показників стану безпеки кожного комп’ютера від стану безпеки, заміряному при його нормальному функціонуванні.

У разі виникнення інциденту, компоненти безпеки, призначені для виявлення аномальної поведінки, подачі сигналів тривоги, реакції на загрози і криміналістичного аналізу порушень безпеки, сповіщають про порушення адміністратора, визначають інцидент, аналізують його та надають свій журнал реєстрації подій. Ознаки інциденту діляться на дві основні категорії: повідомлення про те, що інцидент відбувається зараз, і повідомлення про те, що інцидент, можливо, відбудеться в недалекому майбутньому.

Щоб підвищити ефективність процесу управління інцидентами, необхідно визначити показники ефективності, що залежить від:

- координації і узгодженості дій всіх залучених у процес осіб;
- наявних можливостей з отримання і аналізу інформації, пов'язаної з інцидентом;
- оперативності і коректності отриманих результатів.

Застосування інтелектуальних технологій в управлінні інцидентами ІБ повинно дати поштовх до ефективності управління цим процесом. В якості базових можна виділити чотири інтелектуальні технології: технологія експертних систем, технологія нечіткої логіки, технологія нейромережних структур, технологія асоціативної пам’яті [4]. Саме технологія підтримки прийняття рішень у поєднанні з технологією експертних систем є найбільш актуальними у сфері ІБ завдяки своїй здатності допомагати адміністратору приймати рішення відповідно до інциденту.

Якщо після аналізу виявилося, що інцидент впливає на систему, наступним кроком буде звернення до інтелектуальної системи. На цьому етапі сигнатури вхідного інциденту будуть порівнюватися з сигнатурами вже наявних інцидентів у базі знань, кожному з яких однозначно відповідає певна гіпотеза з поясненнями наступних дій адміністратора.

В якості інтелектуальної системи пропонується інформаційна система підтримки прийняття рішень (ІСППР), яка може працювати за наступним алгоритмом:

1. Оперативні дані сенсорів безпеки аналізуються та оцінюються на предмет наявності сигнатур відомих інцидентів за допомогою бази знань ІСППР.

2. ІСППР на підставі аналізу надає інструкцію щодо усунення причин і наслідків інциденту ІБ, якщо його сигнатура наявна у базі знань.

3. Якщо виник інцидент, сигнатури якого немає у базі знань, то ІСППР дає декілька гіпотез відносно подальших дій адміністратора ІБ.

4. Необхідно виконати дії щодо запобігання повторного виникнення інциденту ІБ. Доцільно, щоб алгоритм роботи інтелектуальної системи щодо керування інцидентами ІБ вписувався в цикл моделі безперервного поліпшення управління процесами PDCA.

Отже, було представлено у якості інтелектуальної системи – ІСППР у сфері інцидентів ІБ в організаційно-технічних системах. При використанні процесного підходу, визначеного у відповідних міжнародних стандартах ISO/IEC, дана схема цілком вписується в модель PDCA.

Таким чином, питання підтримки прийняття рішень є досить важливим в контексті прийняття рішень у сфері інцидентів ІБ, його можна розглядати як частину більш загальної проблеми підтримки прийняття управлінських рішень у кризових ситуаціях. Визначено головні чинники, критерії і показники автоматизованих процедур підтримки прийняття рішень у сфері управління інцидентами ІБ. За вдалого налаштування ІСППР, особа, що уповноважена приймати рішення щодо інцидентів ІБ, буде мати у своєму розпорядженні декілька гіпотез, до яких будуть відноситися певні дії на етапі реагування, а також фундаментальну теоретичну основу для прийняття оптимальних рішень, аби якнайшвидше ліквідувати наслідки та максимально мінімізувати втрати, тому дослідження даного наукового напрямку вважаємо актуальним та перспективним.

Література

1. Толюпа С.В. Проектирование систем поддержки принятия решений в процессе восстановления и обеспечения комплексной защиты в информационных системах. // Науково-технічний журнал “Сучасний захист інформації”.– 2012. - №4. – С. 69-74.
2. Куканова Н. Управление инцидентами информационной безопасности // Открытые системы. — 2006. — № 10. — Електронний ресурс.
3. Стандарт ISO/IEC TR 18044:2004 "Менеджмент інцидентів інформаційної безпеки"
4. Гладиш С.В. Підтримка прийняття рішень щодо керування інцидентами інформаційної безпеки в організаційно-технічних системах. Експертні системи та підтримка прийняття рішень. с. 116-124.

УДК 004.415.056.5

ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ ВІД ВНУТРІШНІХ ЗАГРОЗ

Дмитрук В.Р., Толюпа С.В.
Київський національний університет імені Тараса Шевченка, м. Київ
E-mail: vladislava.dmitruk@gmail.com

Protection of information resources against internal threats

Analysis of security mechanisms regarding insider attacks in modern information systems is conducted. The main tasks and functions of Information Protection and Control (IPC) technology are examined. Information security system from insider threats includes technical security mechanisms and software, psychological and organizational measures and work with staff. In order to ensure and develop comprehensive security system creating of the appropriate unit to adress internal threats, developing enterprise security policies and implementing continuous security monitoring are proposed.

Процеси глобалізації та інформатизації відіграють важливу роль у діяльності кожного підприємства. Створення електронних архівів та масивів даних стає, з одного боку, необхідно умовою підвищення ефективності роботи кожного підприємства, а з іншого – джерелом нових небезпек. Так, згідно за статистикою, станом на 2015 рік співвідношення інцидентів інформаційної безпеки, що виникло через внутрішні загрози, до інцидентів, пов’язаних з зовнішніми джерелами загроз, тримається на рівні 65% до 35% відповідно.

Інсайдер - робітник компанії, який має доступ до конфіденційної інформації, розміщеної у комп'ютерній мережі установи. Внутрішні порушники поділяються на наступні категорії: лояльні інсайдери (недбалі та маніпульовані); скривджені та нелояльні інсайдери; мотивовані ззовні (мотивовані фінансово та впроваджені); інші порушники (ті, що мають на меті вплинути на вартість акцій підприємства) [1].

Протидія інсайдерству має здійснюватися безперервно, адже кожен співробітник, який має доступ до інформації є потенційним порушником. При цьому необхідно дотримуватись балансу між закритістю інформації та її доступністю для працівників компанії, інакше вони не зможуть виконувати свої прямі обов’язки. Основні напрямки захисту від інсайдерів [2]: захист документів; захист каналів витоку; моніторинг дій користувачів.

Information Protection and Control (IPC) – технологія захисту конфіденційної інформації від внутрішніх загроз. Рішення класу IPC призначені для захисту інформації від внутрішніх загроз, запобігання різних видів витоків інформації, корпоративного шпигунства і бізнес-розвідки. У цій системі комбінується два основні підходи до захисту: шифрування носіїв даних у всіх вузлах мережі та здійснення контролю за технічними каналами витоку інформації із залученням технологій DLP.

До додаткових завдань цієї системи належать:

- запобігання передачі зовні не тільки конфіденційної, а й іншої небажаної інформації;

- запобігання передачі небажаної інформації не тільки зсередини назовні, але і зовні всередину інформаційної системи організації;

- запобігання використання працівниками Інтернет-ресурсів та ресурсів мережі в особистих цілях;

- захист від спаму та вірусів;

- оптимізація завантаження каналів, зменшення нецільового трафіку;

- облік робочого часу і присутності робітників на робочому місці;

- архівування інформації на випадок випадкового видалення або псування оригіналу;

- захист від випадкового або навмисного порушення внутрішніх нормативів;

- забезпечення відповідності стандартів в області інформаційної безпеки і чинного законодавства.

IPC – системи використовують DLP-системи для здійснення контролю за потоками інформації, що циркулюють ззовні та у мережі. Основним завданням DLP-систем, є запобігання передачі конфіденційної інформації за межі інформаційної системи. Така передача (витік) може бути навмисною або ненавмисною. Як показує практика, більша частина витоків відбувається не через зловмисні наміри, а через помилки, неуважність, безтурботність, недбалість працівників. Інша частина пов'язана зі злим умислом операторів і користувачів ІС. Зрозуміло, що інсайдери, як правило, намагаються подолати засоби DLP-систем. Результат цієї боротьби залежить від багатьох факторів. Гарантувати успіх тут неможливо.

Технології IPC використовують різні підключаються криптографічні модулі, в тому числі найбільш ефективні алгоритми DES, Triple DES, RC5, RC6, AES, XTS-AES.

Технологія DLP в IPC підтримує контроль наступних технічних каналів витоку конфіденційної інформації: периферійні пристрої (USB, LPT, COM, WiFi, Bluetooth і інше); локальні і мережеві принтери; корпоративна електронна пошта; веб-пошта; соціальні мережі та блоги; файлообмінні мережі, форуми та інші інтернет-ресурси; засоби миттєвого обміну повідомленнями тощо.

Технології DLP в IPC підтримують контроль в тому числі наступних протоколів обміну даними: FTP, FTP-over-HTTP, FTPS, HTTP, HTTPS (SSL), NNTP, POP3, SMTP.

Крім основного перед DLP-системою можуть стояти і вторинні (побічні) завдання. Вони такі:

- архівування повідомлень, які пересилаються на випадок можливих у майбутньому розслідувань інцидентів;

- запобігання передачі зовні не тільки конфіденційною, але і іншої небажаної інформації (образливих виразів, спаму, еротики, зайвих обсягів даних тощо);

- запобігання передачі небажаної інформації не тільки зсередини назовні, але і зовні всередину інформаційної системи;

- запобігання використанню працівниками державних інформаційних ресурсів в особистих цілях;

- оптимізація завантаження каналів, економія трафіку;

- контроль присутності працівників на робочому місці;

- відстеження благонадійність співробітників, їх політичних поглядів, переконань, збір компромату.

Для того, щоб зафіксувати передачу конфіденційної інформації, використовуються такі технології:

1) сигнатури – пошук у потоці даних певної послідовності символів;

2) «цифрові відбитки» (Digital Fingerprints або DG). DLP/IPC-системі передається якийсь стандартний документ-шаблон, з нього створюється «цифровий відбиток» і записується в базу даних DF. Після цього в правилах контентної фільтрації настроюється процентна відповідність шаблону з бази;

3) «мітки». - призначення спеціальних «міток» файлам, що містять конфіденційну інформацію;

4) пошук за регулярними виразами;

5) лінгвістичні методи;

6) ручне детектування («Карантин»).

Однак, жоден з наведених методів детектування конфіденційної інформації не може вважатися цілком надійним. Необхідно комбінувати різні продукти та методи, зважаючи на їхні сильні та слабкі сторони. Загалом система захисту інформації від внутрішніх загроз повинна включати в себе як технічний захист каналів витоку, так і програмні засоби, психологічні та організаційні заходи, і роботу з персоналом.

Спеціалізований структурний підрозділ Державного центру кіберзахисту та протидії кіберзагрозам CERT-UA розробив рекомендації щодо захисту інформаційних ресурсів від внутрішніх загроз. Так, необхідно будувати систему захисту, орієнтуючись на попередній досвід компанії щодо внутрішніх інцидентів ІБ. Перш за все, необхідно забезпечити надійний захист критично важливих ресурсів, для цього необхідно використовувати різноманітні технології та системи захисту (DLP, SIEM, IDS тощо). Для створення системи інформаційного захисту можуть використовуватись такі продукти, як McAfeeDataLossPreventio Host, Reconnex, PortAuthority 5.0, StarForceContentEnterprise. Однак жоден з них не може забезпечити повний захист від діяльності інсайдерів. На думку спеціалістів даної організації, головним індикатором захищеності від внутрішніх загроз є взаємовідносини з партнерами та між співробітниками [3].

Отже, необхідно комплексно забезпечувати та розвивати систему захисту. Для того, щоб забезпечити комплексність ІБ, потрібно сформувати відповідний підрозділ з протидії внутрішнім загрозам, розробити політику безпеки підприємства та впровадити постійний контроль за станом безпеки підприємства. Систему захисту необхідно постійно покращувати та вдосконалювати.

Література

1. Ульянов В.В. Динамика безопасности: от внешних угроз – к внутренним / В.В.Ульянов // Защита информации. INSIDE.– 2008. - № 4. – С. 34 – 38.
2. Probst, C.W. Insider Threats in Cyber Security/ C.W. Probst– 2010. – 245р.
3. CUA-15-04R. Рекомендації CERT-UA з протидії загрозі інсайдера [Електронний ресурс] / І. Соколов - №1 – 2015 - Режим доступу: http://cert.gov.ua/pdf/CUA-15-04R.pdf

УДК 621.391;681.3.06+519.6(075.8)

АНАЛІЗ ПОТОКІВ ВІДМОВ БАГАТОВИМІРНИХ МЕРЕЖ

Федюнін С. А.
Державний університет телекомунікацій, Україна
E-mail: s.fediunin@gmail.com

Failure stream of multidimensional networks.

The problems of construction of multidimensional next generation network are considered. It is shown that main problem for these networks is a creation of a control system, which will have the reliability parameters. Concept of failure stream of restoring system are determined. The basic properties of stationary and non-stationary flows of failures are analyzed.

Сучасні інфокомунікаційні мережі – це не лише мережі транспорту і доступу, але ще і мережі підтримки і сервісу, тобто мережі синхронізації, сигналізації, управління, мережі передачі сигналів часу і тому подібне. Всі вони мають власні технічні і, зокрема, обчислювальні засоби і вирішують з їх допомогою поставлені завдання. В сукупності мережі транспорту, доступу, підтримки і сервісу, зрозуміло, частково взаємодіють між собою, але така взаємодія відбувається лише в міру необхідності і не розглядається як істотний принцип їх розвитку і вдосконалення в умовах автономності існування цих мереж [1]. Тому принцип "багато послуг – одна мережа" не лише в сучасних мережах, але і в мережах NGN (Next Generation Network – мережа наступного покоління) в значній мірі декларативний.

Інша справа – мережі FGN (Future Generation Networks – мережі майбутніх поколінь). Передбачити їх архітектуру і навіть загальні принципи побудови дуже важко, але все таки аналіз тематики деяких сучасних теоретичних досліджень в області складних систем і всіляких мережевих структур дозволяє зробити деякі припущення про можливу подобу і навіть деякі особливості мереж майбутнього. Є підстава вважати, що це будуть багатовимірні мережі [2]. До питань теорії побудови такого роду мереж в різних областях природознавства і, у тому числі, в області телекомунікацій останніми роками виявляється значний інтерес.

Багатовимірність інфокомунікаційної мережі. Відомо, що багатовимірність, що розглядається як конструктивний принцип, є способом об'єднання розрізнених шляхів в єдине ціле і, відповідно, багатовимірні мережі майбутнього не обов'язково повинні мати чітко виражене ділення на мережі транспорту, доступу і згадані мережі підтримки і сервісу[2, 3]. Тому в мережах FGN, тобто в інфокомунікаційних мережах майбутнього, стане можливим за рахунок використання багатовимірної структури мережі і багатоядерних обчислювальних засобів в її вузлах забезпечувати обмін інформацією і надання всіляких послуг споживачам по майже примітивній, на перший погляд, схемі:

Споживачі (Користувачі) – Багатовимірна мережа – Споживачі (Користувачі)

При такому підході доступ, транспорт, сервіс, підтримка (синхронізація, сигналізація і т. д.) – це внутрішня справа інтегрованої мережі FGN,

багатовимірна архітектура якої в принципі надає можливості спільного вирішення завдань, покладених на складові її мережі, у тому числі неординарними способами, відповідними рівню винаходів.

Можна передбачити, що для мережі майбутнього FGN найпростіше рішення, при якому мережі доступу, транспорту і різні мережі підтримки знаходяться в своїх власних, лише для них відведених, вимірах навряд чи буде кращим рішенням. Між іншим, по суті, хоч і з деякою натяжкою, таке положення якраз має місце зараз, якщо, наприклад, існуючу мережу загального користування розглядати теж як багатовимірну мережу, де в своїх власних вимірах знаходяться: транспорт, доступ і різні мережі підтримки і сервісу.

Навпаки, в мережі FGN, при її спочатку і принципово багатовимірній структурі можна буде використовувати загальні ресурси цієї мережі і особливо обчислювальні ресурси різними, а, можливо, і всіма підмережами цією багатовимірної і, як правило, багаторівневої мережі.

Відповідно перехід до багатовимірних мереж з максимальним використанням ресурсів, що є у них, може розглядатися як вельми істотний, якщо не головний, показник відмінності мереж FGN від сучасних мереж, у тому числі мереж NGN.

Основною проблемою для цих мереж є створення системи управління, яка буде мати визначені параметри надійності. Як відомо, основою створення надійних систем є забезпечення властивості відновлення після відмов.

Основні властивості потоків. Потік називають стаціонарним, якщо закон розподілу вектору числа відмов $\eta(a+t_1)–\eta(a)$, $\eta(a+t_2)– \eta(a)$, …… , $\eta(a+t_d)–\eta(a)$ відповідно на відрізках часу (a, $a+t_1$;a, $a+t_2$;…; a, $a+t_d$) залежить тільки від тривалості цих відрізків t_1, t_2, … , t_d, але не залежить від вибору загального моменту а початку відрізків. В іншому випадку потік називають нестаціонарним. Виконання вимог стаціонарності означає що ймовірні характеристики потоку не залежать від часу. Зокрема, закон розподілу числа відмов на будь-якому проміжку часу (t_1, t_2) не залежить від самих значень t_1 і t_2, а залежить тільки від їх різниці $t_2–t_1$.

На осі часу виділимо набір непересічних проміжків часу довжиною Δt_1, Δt_2, … , $\Delta t_к$ (Рис.2) і позначимо через $\Delta\eta_1(\Delta t_1)$, $\Delta\eta_2(\Delta_2)$, …, $\Delta\eta_к(\Delta t_к)$ випадкові величини – числа відмов на цих проміжках часу.

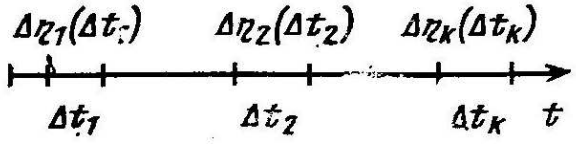


Рис. 2. До визначення поняття «післядія в потоці відмов»

Потік відмов називають *потоком без післядії*, якщо для будь-якого набору непересічних проміжків часу Δt_1, Δt_2, …, $\Delta t_к$ числа відмов на цих проміжках $\Delta\eta_1(\Delta t_1)$, $\Delta\eta_2(\Delta t_2)$, …, $\Delta\eta_к(\Delta t_к)$ являють собою взаємно незалежні випадкові величини. Тому, якщо маємо k непересічних проміжків часу Δt_1, Δt_2, …, $\Delta t_к$ і ймовірність виникнення n_1, n_2, …, k відмов протягом кожного з цих проміжків

відповідно дорівнюють $p(n_1,\Delta t_1)$, $p(n_2,\Delta t_2)$, …, $p(n_k,\Delta t_k)$, то ймовірність поєднання подій (протягом відрізку часу Δt_1 виникає n_1 відмов, протягом відрізку часу Δt_2 виникає n_2 відмов і т.д.) дорівнює похідній ймовірності

$$\prod_{i=1}^{k} p(n_1, \Delta t_1)\, p(n_2, \Delta t_2) \ldots\ p(n_k, \Delta t_k)$$

Зокрема, виконання вимоги відсутності наслідку означає, що розподіл числа відмов на будь-якому проміжку часу не залежить від реалізації потоку до та після цього проміжку часу.

Потік називають *ординарним* якщо

$$\lim_{\Delta t \to 0} \frac{q(2, \Delta t)}{\Delta t} = 0,$$

де $q(2, \Delta t)$ – ймовірність виникнення меншою мірою двох відмов протягом проміжку часу довжиною Δt.

Ординарність означає практичну неможливість виникнення двох чи більше відмов одночасно.

Введемо деякі додаткові поняття. Провідна функція потоку визначається як математичне очікування числа відмов за час t:

$$W(t) = M[\eta(t)].$$

Очевидно, що $W(t)$ – ненегативна неубутна функція. Ця функція до того ж практично завжди диференційована, та існує величина

$$\omega(t) = \frac{dW(t)}{dt},$$

яку називають *параметром потоку відмов*.

Очевидно, що у стаціонарного потоку параметр $\omega(t)=\omega$, тобто є постійною величиною та не залежить від часу. Провідна функція при цьому являється лінійною функцією часу, тобто $W(t)= \omega t$.

Література

1. Битнер В. Н. Сети нового поколения – NGN : учебное пособие для ВУЗов / В. Н. Битнер, Ц. Ц. Михайлова. – Москва : Горячая линия – Телеком, 2011. – 226 с.
2. Коновалов Г. В. Многомерные сети как философия сетей FGN // Материалы VII международной научно-технической конференции «Перспективные технологии в средствах передачи информации — ПТСПИ’2007». 10-12 октября 2007. – Владимир: – 2007.
3. Bhushan N. Network densification: the dominant theme for wireless evolution into 5G/ N. Bhushan, Li Junyi, D. Malladi et al. // IEEE Communications Magazine. USA: Institute of Electrical and Electronics Engineers. – 2014. – Vol. 52, No. 2. – P.82-89.

УДК 355.48

ВИМОГИ ДО СИСТЕМИ ПРОТИДІЇ НЕГАТИВНОМУ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОМУ ВПЛИВУ

Міхєєв Ю.І., Чернявський Г.П., Пінчук О.І., Шапар М.В.
Житомирський військовий інститут імені С. П. Корольова, Україна
E-mail: yuramiheev@ukr.net

System of counteraction to negative informatively-psychological influence

In article the presented variant of creation of the system of counteraction to negative informatively-psychological influence. The structure of the system and task of her subsystems is presented. System requirements are pointed such to the type and the stages of her creation.

Швидкий розвиток інформаційно-телекомунікаційних технологій зумовив появу інформаційного простору із новими комунікаційними можливостями. Це спричинило виникнення нових загроз національній безпеці держави. Так, подання та розповсюдження спеціально підготовленої інформації в засобах масової комунікації під виглядом новин переводять її в розряд прихованого негативного інформаційно-психологічного впливу (ІПсВ) [1]. Одним з наслідків дії ІПсВ може стати прийняття хибних рішень та втрата довіри до керівництва держави як окремою особою, так і всім населенням країни. Запобігти можливим наслідкам, спричиненим ІПсВ, можливо лише завдяки створенню надійної системи попередження та захисту від зовнішніх інформаційних загроз, яка повинна передбачати появу негативного впливу, визначати ступінь його загрози, здійснювати нейтралізацію та надавати пропозиції щодо подальшого розвитку ситуації представникам відповідних державних органів та відомств.

У доповіді наведено варіант структури перспективної системи протидії негативному ІПсВ (рис. 1), розглянуто етапи її створення. Зазначено, що система протидії негативному ІПсВ повинна складатися із підсистем моніторингу інформаційного простору та визначення рівня негативного ІПсВ, спрямованого на свідомість особи, яка приймає рішення.

У зв’язку з тим, що сьогодні наявний інформаційний простір у своїй більшості представлений ресурсами Інтернет, підсистема його моніторингу повинна охоплювати всі можливості щодо пошуку інформації, а саме [2]: пошукові системи, тематичні каталоги ресурсів, сайти новин, RSS-повідомлення, інформаційні агентства, які здійснюють он-лайн відеотрансляцію новин з урахуванням їх особливостей щодо висвітлення інформації. Тому необхідним етапом при створенні даної підсистеми є формування бази даних пошукових ресурсів, наявних в Інтернеті. Список інформаційних ресурсів повинен формуватися таким чином, щоб вони, доповнюючи один одного, максимально охоплювали інформацію за даною темою у відповідно до встановлених пошукових обмежень.

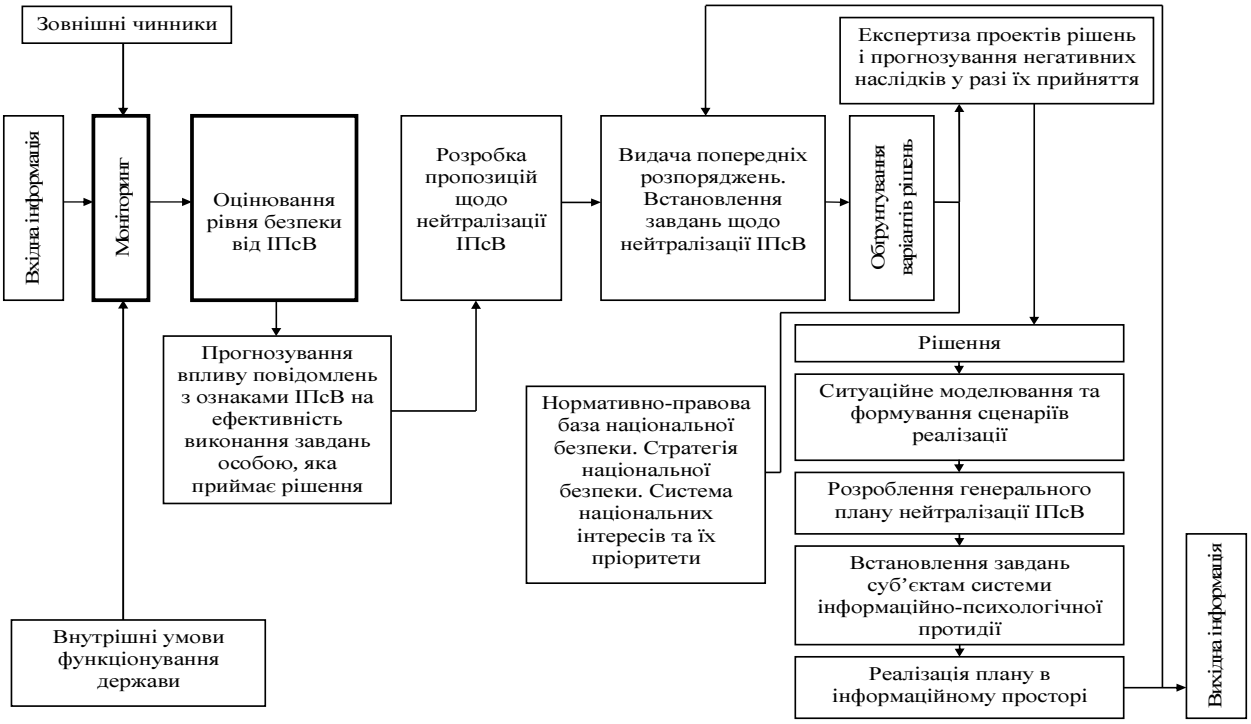


Рис.1. Структура перспективної системи протидії негативному ІПсВ

Подальша робота системи повинна бути пов'язана з обробкою знайденого матеріалу. При вирішенні даного завдання необхідною є організація автоматичного реферування знайденої інформації.

Для візуалізації знайденої інформації з метою її подальшого аналізу доцільно скористатися технологією побудови семантичних мереж. Порівняння семантичних мереж різних текстів дозволяє встановити ступінь їх змістової близькості, що може використовуватися для автоматичної класифікації документів за заданими рубриками, їх пошуку за подібністю заданого тексту, а також розбиття інформаційного масиву на класи документів близького змісту [3].

Основні етапи створення підсистеми визначення рівня негативного ІПсВ повинні передбачати наявність компетентних експертів у цій галузі знань. На основі статистичної обробки даних, отриманих за результатами моніторингу інформаційного простору, у подальшому можливо встановити значення періодів спостереження та визначити для них відповідні критерії рівня ескалації загального негативного ІПсВ відносно визначеної групи осіб. Результати оцінювання повинні стати підґрунтям для розробки рекомендацій щодо дій в умовах негативного ІПсВ.

Таким чином, поєднавши функції та завдання двох підсистем в умовах сучасного інформаційного простору, перспективна система протидії негативному ІПсВ повинна забезпечити:

- періодичний автоматизований збір та тематичний пошук документів у відкритих джерелах інформації;

- автоматичну та автоматизовану обробку текстових документів, виділення з них об'єктів інтересу та пов'язаних з ними фактів;

- класифікацію різномовних текстів за єдиними критеріями;
- автоматичну лінгвістичну обробку;
- відбір відомостей з банку текстової інформації або з бази знань за вимогами оператора;
- інтегрування та узагальнення знань, які містяться в різномовних текстах з певної предметної галузі;
- перевірку даних, які містяться в різномовних текстах та в їх сукупності, на наявність дезінформації;
- виявлення закономірностей у певній предметній галузі та їх формування на змістовому рівні;
- збереження в базі даних отриманої інформації, а також надання авторизованого доступу користувачів до перегляду та аналітичної обробки документів;
- створення єдиного структурованого архіву об'єктів інтересу, досьє на них, а також подій та взаємовідношень між ними з метою моніторингу змін їх стану в процесі діяльності, виконання часових, географічних та тематичних зрізів при формуванні різноманітних звітів;
- надання аналітикам засобів швидкого виявлення неявних зв'язків між об'єктами моніторингу та пов'язаними з ними фактами й подіями;
- візуалізацію результатів аналітичних досліджень шляхом генерації дайджестів статей та фактів, формалізованих досьє, семантичних мереж та інших аналітичних звітів;
- визначення рівня інформаційної загрози від негативного ІПсВ;
- розроблення варіантів нейтралізації негативного ІПсВ;
- можливість вибору оптимально варіанта нейтралізації негативного ІПсВ за обраним критерієм;
- прийняття рішення про нейтралізацію негативного ІПсВ;
- підготовку та всебічне забезпечення реалізації рішення;
- нейтралізацію негативного ІПсВ;
- оцінювання рівня інформаційної загрози після впливу на неї системи протидії негативному ІПсВ.

Література

1. Брайант Д. Основы воздействия СМИ / Д. Брайант, С. Томпсон; пер. с англ. – М. : Изд. дом "Вильямс", 2004. – 432 с.
2. Системы мониторинга и анализа СМИ [Электронный ресурс]. – Режим доступа: http://www.newart.ru/oparin/smi_oparin.htm.
3. Michael W. Berry. Survey of Text Mining. Clustering, Classification and Retrieval Michael W. Berry. – Springer-Verlag, 2004. – 244 p.
4. Хан У. Системы автоматического реферирования [Электронный ресурс] / У. Хан, И. Мани // Открытые системы. – 2000. – № 12. – Режим доступа: http://www.osp.ru.

УДК 004.75

ИСПОЛЬЗОВАНИЕ ОБЛАЧНЫХ ТЕХНОЛОГИЙ В КОНТЕКСТЕ НОВЫХ УСЛУГ В 3G СЕТЯХ ОПЕРАТОРОВ МОБИЛЬНОЙ СВЯЗИ

Вдовенко Е.А., Воропаева А.А., Игнатьева В.Ю.
Донецкий национальный технический университет, Украина
E-mail: l.vdovenko@mail.ru

The use of cloud computing in the context of new services in 3G networks

The article describes the advantages of using cloud technologies in 3G-networks and shows some examples of services that solve the problem of lack of free space on mobile devices.

Широкомасштабное внедрение услуг 3-го поколения мобильной связи позволяет мобильным операторам намного увеличить и разнообразить список предоставляемых услуг, что повлечет за собой увеличение прибыли и абонентской базы. Однако для расширения своих возможностей и улучшения качества связи, операторам требуется мощное оборудование, способное обрабатывать такой поток данных. Решением данной проблемы являются центры обработки данных (ЦОД). ЦОД – это высокопроизводительная вычислительная система для решения наборов простых задач по последовательным алгоритмам и сложных задач по параллельным алгоритмам.

Благодаря дата-центрам открывается наиболее обширная и прибыльная область IT-услуг – внедрение облачных технологий. Это очень разноплановая и перспективная отрасль, которая приобретает всё большую популярность. Так, согласно проведенного опроса, в ходе которого в течении недели нами было опрошено 445 респондентов со всей Украины, 42% опрошенных уже используют облачные хранилища [1].

Характеристики сегодняшних облачных вычислений с учетом их особенностей определены в стандартах NIST (Национальный институт стандартов и технологий США) в следующем: самообслуживание по требованию (англ. self-service on-demand), универсальный доступ по сети, объединение ресурсов (англ. resource pooling), эластичность и учет потребления [2].

Различают «облака» в зависимости от формы предоставления услуг – публичные, частные и гибридные. Публичные «облака», в основном, применяются в повседневной жизни, где нет необходимости в конфиденциальности информации, частные – в локальной корпоративной сети, а гибридные – одновременно используют и публичные и частные «облака».

Внедрение оператором мобильной сети услуги облачного хранилища для своих пользователей, выгодна как оператору, так и абонентам. Оператор предоставляет тариф, в абонплату которого включена стоимость пользования облачным хранилищем, дополнительная плата за передачу данных не взымается. Изначально предоставляется некоторый объем хранилища, который при желании пользователь может расширить за дополнительную плату. Однако, чтобы данная услуга была конкурентоспособной на рынке, необходимы дополнительные опции, которые смогут привлечь большее количество клиентов.

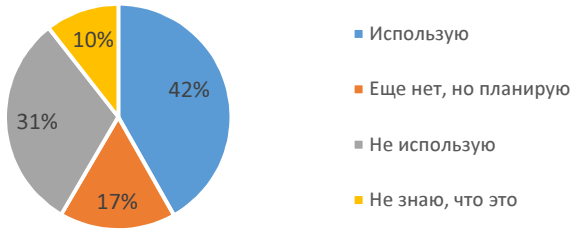


Рис. 1. Тенденции использования облачных технологий пользователями.

С целью определения какие услуги больше всего интересуют мобильных пользователей мы провели опрос, в результате которого выяснили что, доминирующая операционная система – Android; степень использования онлайн сервисов высокая, причем лидируют социальные сети, аудио- и видео-онлайн; большая часть респондентов испытывает проблемы с нехваткой свободного места на устройстве (более 60%), причем хранения фото и аудио приоритетнее чем хранение видео. Поэтому мы решили остановится именно на проблеме нехватки свободного объема памяти.

Как решение данной проблемы, мы выбрали способ сохранения данных напрямую в облако, обходя память устройства. Это касается не только файлов, скачанных из сети, но и фотографий, сделанных данным устройством.

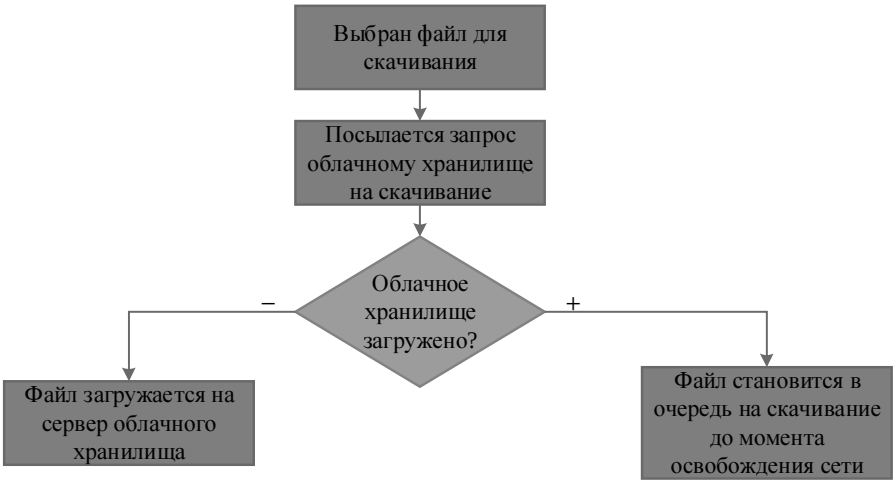


Рис. 2. Алгоритм работы функции скачивания файлов напрямую в облачное хранилище.

Первая предлагаемая нами функция – это сохранение файлов из сети напрямую в облако. Пользователю не нужно будет проделывать бесполезный и времязатратный алгоритм действий: скачать файл на устройство, сбросить его в облачное хранилище, а затем удалить. Также для этого процесса всё-таки необходим свободный объем памяти на устройстве. При наличии указанной функции, пользователю нужно будет только скопировать сетевой адрес архива, музыкального трека, документа, картинки или даже веб-страницы, поместить его в отведенном месте в приложении оператора и, спустя короткий промежуток

времени, необходимая информация будет сохранена в указанном пользователем «облачном» месте.

Выгода предоставления данной функции мобильным оператором не только материальная, так же она поможет значительно разгрузить транспортную сеть.

Вторая функция – хранение фотографий в «облаке», а на самом устройстве только превью фотографий. То есть на мобильном устройстве будут храниться фотографии в низком качестве лишь для отображения их предпросмотра. Но как только пользователь нажмет на фото—оно будет тут же скачано в оригинале из «облака». Это весьма удобный функция, пользователь может продолжать фотографировать сколько угодно, оригиналы хранятся в «облаке», а его смартфон останется свободен для новых снимков.

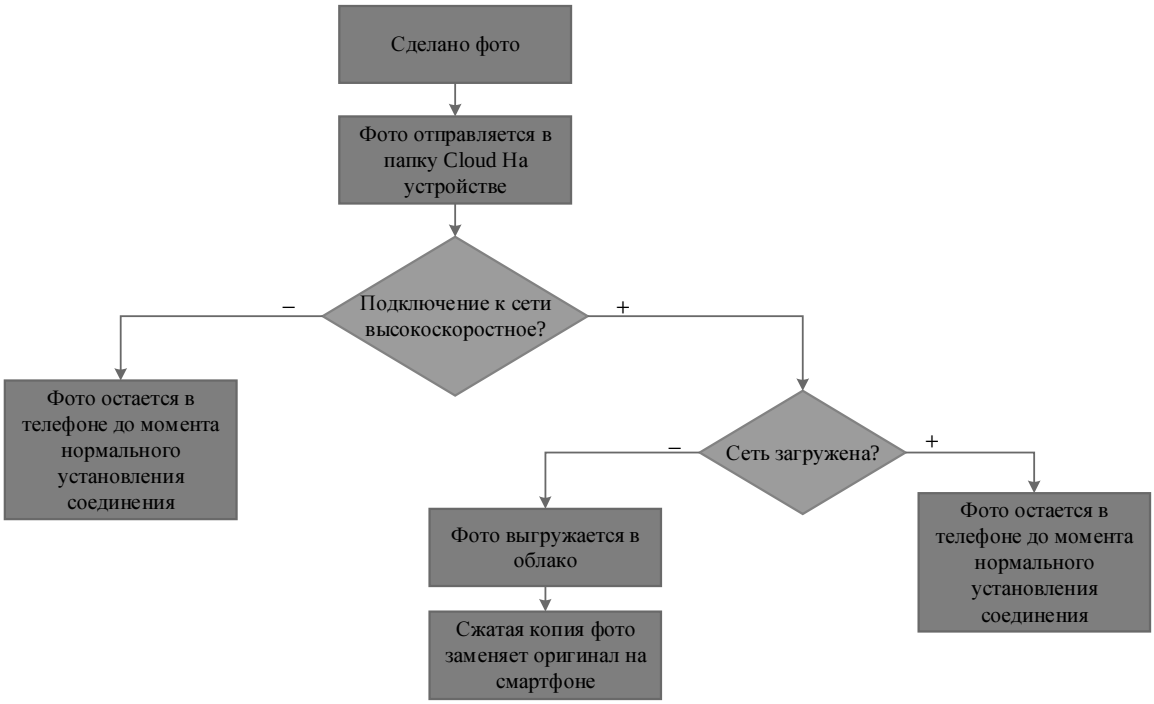


Рис. 3. Алгоритм работы функции «Хранение фото в облаке».

Данные функции имеют аналоги в сервисах Google, но предоставление их конкретно операторами связи сможет обеспечить снижение трафика магистральных сетей, так же будет выгодным и удобным для клиентов, что будет способствовать увеличению спроса на данную услугу, а с ним и увеличение прибыли.

Дальнейшие исследования будут направлены на разработку приложения, включающего указанные опции.

Литература

1. Соцопрос: Насколько Вы используете возможности Вашего смартфона? [Электронный ресурс]. – Режим доступа: https://goo.gl/SF9nVa
2. С. С. Баранова Исследования тенденций развития облачных сервисов // Cloud of science . 2014. №3 С.517-523.
3. Монахов Д. Н., Монахов Н. В.Облачные Технологии. Теория и практика/МАКС Пресс Москва, МГУ,2013–128с.

УДК 004.78: 007

ДОСЛІДЖЕННЯ МОДЕЛІ ПОТОЧНОГО СТАНУ КОМПОНЕНТІВ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Шевченко О.В.
Тернопільський національний технічний університет ім. І. Пулюя, Україна
E-mail:Shevchenko_Sasha_2@ukr.net

RESEARCH A MODEL THE CURRENT STATE OF THE MOBILE COMPUTER NETWORK

Investigate the model of the current state of the mobile network components in real time. Formulates the task of developing of the algorithm the mobile network.

Постановка задачі:

Параметри роботи комп'ютерної мобільної мережі (КММ) забезпечуються інформацією про стан системи у процесі її функціонування. Це досягається безпечним з'єднанням системи управління КММ з її компонентами, і вимагає вирішення таких задач:

- моніторингу стану КММ відповідно до вибраної стратегії;
- накопичення даних, що відображають події, які відбуваються у КММ;
- реалізацію технологічних, обслуговуючих процесів зворотного зв'язку;
- прогноз змін та подій, що можуть відбуватись у КММ;
- використання загальної моделі функціонування КММ.

КММ функціонує як система, що розподілена у просторі і часі, і це накладає додаткові вимоги методи розв`язку задач, які забезпечують функціонування КММ, а саме:

- формування значень параметрів КММ за параметрами її компонентів;
- обчислення параметрів, які враховують особливості, що є характерними для КММ;
- управління КММ, яке забезпечує вплив на зміну величин параметрів;
- здійснення фрагментації КММ у залежності від поточного стану фрагментів мережі;
- вирішення проблеми міграції подій у КММ.

Вирішення задачі:

Виходячи з того, що КММ є системою розподіленою на модель управління і модель траєкторії руху повідомлення, необхідно сформувати параметри в межах окремих вузлів КММ, які будуть визначаються такими критеріями, як надійність, швидкість передачі повідомлення, безпека

передачі повідомлення, кожний з яких будемо позначати наступними символами: η, υ, λ, відповідно. Засоби, які забезпечать величини значень цих параметрів, є показниками якості обслуговування, позначається $\pi = f(\eta, \upsilon, \lambda)$. Величини цих затрат будемо позначати C^{η}, C^{υ}, C^{λ}, які являють собою функцію відповідного параметра якості, що записується у вигляді:

$$C^{\eta} = f^{\eta}(\eta); \quad C^{\upsilon} = f^{\upsilon}(\upsilon); \quad C^{\lambda} = f^{\lambda}(\lambda). \tag{1}$$

Виходячи з значення параметру якості π сформуємо значення параметрів фрагментів КММ.

Стійкість КММ можна забезпечити вимогами надійності, що характеризує здатність системи виконувати функції, визначені технічними вимогами.

Враховуючи те, що задача забезпечення параметрів надійності не має рішення завдяки складності з забезпеченням адекватного управління рівнем надійності, у цьому випадку стоїть питання про забезпечення гарантії передачі повідомлення ω_i. Розв`язок задачі полягає у підключенні до всіх засобів, що беруть участь у передачі повідомлення.

Завдяки цьому розподіл системи на окремі фрагменти є актуальним, оскільки разом з цим відпадає необхідність управління параметрами π, і визначення компонентів управління КММ. Принцип полягає у тому, що при черговій зміні фрагментації у новий фрагмент попадають елементи КММ, які забезпечують рівень значення параметрів якості.

Моніторинг КММ здійснюється зворотнім зв`язком між елементами КМ та системою управління.

Висновок:

Реалізація зворотного зв`язку у КММ здійснюється шляхом накопичення даних і дозволяє реалізовувати процеси управління КММ на основі використання статистичних моделей аналізу.

Такий процес є реалізацію надання послуг на передачу повідомлення ω_i, що здійснює безпечну взаємодію між вузлами КММ на основі використання моделі прогнозування, яка істотно наближена до підходу, який ґрунтується на використанні статистичних методів, а саме:

- функціонування моделі прогнозування ґрунтується на використанні статистичних даних про об`єкт і параметри;
- точність прогнозу окремих параметрів на основі статистичних оцінок;
- використання моделей прогнозування залежить від особливостей об`єкту і процесів.

Відмінність моделі прогнозування від статистичної моделі полягає у тому, що модель прогнозування можна формувати на основі інших формальних засобів, а підвищення точності прогнозування можна забезпечити модифікацією самої моделі, на основі якої будується модель регресії.

Одна з таких моделей використовує логіко-ймовірнісній механізм аналізу стану оцінки системи. Формально вона описується у такому вигляді:

$$\mathrm{H}_1^{LG} = F[L, G] = \{[(x_{2s}, \ldots, x_{2m}) = L_1(x_{1s}, \ldots, x_{1n})]\} \to \ldots \to \{[(x_{n1}, \ldots, x_{nk}) = L_n(x_{(n-1)1}, \ldots, x_{(n-1)g})] \,\&\, \ldots \,\&\, [(x_{(n+k)1}, \ldots, x_{(n+k)m}) = L_{n+k}(x_{(n+k-1)1}, \ldots, x_{(n+k-1)r})]\} \quad (2)$$

Опис компоненти H^{LG} відображається фрагментом відповідного графа.

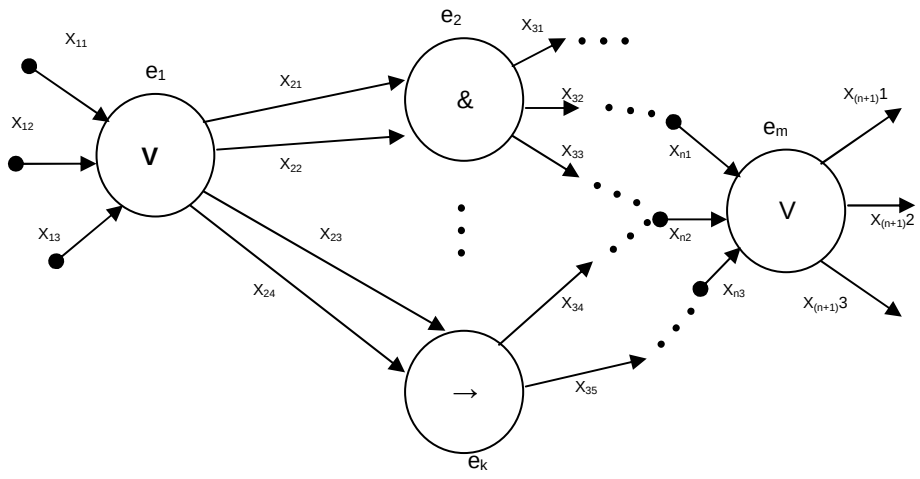


Рис. 1. Фрагмент логіко-графічного образу подій, що відбуваються у КМ.

Вершини графу $e_1 e_2 \ldots e_k \ldots e_m$ ідентифікують елементарні логічні функції, які можуть виконуватися над вхідними параметрами, що позначаються змінними x_{ij}. Індекс «i» позначає порядковий рівень ієрархії графу, індекс «j» означає номер змінної на відповідному рівні ієрархії.

Література

1. Берж К. Теория графов и её применение / К. Берж – ИЛ. – Москва : 1962, – 319 с.
2. Булинская Е.В. Теория риска и перестрахование. Часть I. Упорядочивание рисков / Е.В. Булинская – МГУ. – Москва : 2001. – 119 с.
3. Гольдштейн Б.С. Сигнализация в сетях связи / Б.С. Гольдштейн – Т.1. Радио и связь. – Москва : 2001. – 448 с.

УДК 621.3

ИСПОЛЬЗОВАНИЕ ВИРТУАЛИЗАЦИИ В ЗАДАЧАХ ОПРЕДЕЛЕНИЯ ПАРАМЕТРОВ ПРОИЗВОДИТЕЛЬНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

Сиренко А.И.

Одесская национальная академия пищевых технологий, Украина

E-mail: olexandr.sirenko@gmail.comLiaoning

Using virtualizaton in determination of parameters of computer systems performance

The paper studies a determination of performance parameters for computer systems. The existing approaches and the related problems was described. The dependence of performance parameters on hardware was noted. Using the virtualization technology for limit computer systems hardware resources and find statistical dependence of performance parameters was offered.

При проектировании и анализе функционирования компьютерных систем (КС) важным вопросом является определение параметров производительности при заданном наборе доступных аппаратных ресурсов. Планирование развития КС в большинстве случаев связано с определением качества работы сервисов, предоставляемых КС. Важным вопросом является прогнозирование работы КС с учётом роста нагрузки, увеличением числа клиентов. Анализ параметров производительности позволяет определить необходимые изменения в аппаратных ресурсах КС для обеспечения заданного уровня качества работы сервисов.

В работах, посвящённых вопросам анализа и планирования производительности КС, рассматриваются модели производительности КС [1-2]. Рассматриваемые модели используют аналитическое и имитационное моделирование. Однако следует отметить, что современные сервисы имеют сложную структуру программного и аппаратного обеспечения. Это приводит к усложнению моделей производительности КС, либо увеличению погрешности результатов моделирования.

Одним из подходов, позволяющих определить параметры производительности, является испытания на реальных КС. При этом подходе в сериях наблюдений изменяется аппаратное обеспечение КС и изучается эффект от этого изменения. Данный подход позволяет получить достоверные результаты в виде статистических данных зависимости параметров производительности КС от аппаратных ресурсов. Такой подход является трудоёмким, так как он требует наличия множества вариантов комплектующих аппаратного обеспечения, что в большинстве случаев является экономически нецелесообразным.

Таким образом, поиск методов, позволяющих получить статистическую

информацию о параметрах производительности КС и их зависимости от аппаратных ресурсов, является важной и актуальной задачей.

Одной из технологий, позволяющих гибко изменять аппаратные ресурсы КС в процессе определения параметров производительности, является технология виртуализации [3]. С помощью технологии виртуализации становится возможным поместить исследуемый сервис в виртуальную КС. Аппаратные ресурсы, выделяемые для виртуальной КС, возможно менять в пределах наличия аппаратных ресурсов на основной КС, которая поддерживает работу виртуальных КС. Такой подход позволяет проводить испытания, меняя аппаратные ресурсы исследуемой КС. В ходе испытаний измеряются численные значения параметров производительности при разных характеристиках аппаратных ресурсов.

Полученные таким методом численные значения параметров могут быть использованы для построения статистической модели производительности КС [4]. Статистическая модель позволяет установить количественную взаимосвязь показателей производительности и аппаратных ресурсов КС.

На сегодняшний день существует несколько реализаций технологий виртуализации. К основным реализациям, которые широко используются,можно отнести следующие:

1. VMware [5];
2. Xen [6];
3. KVM [7];
4. VirtualBox [8];
5. Hyper-V [9].

В существующих работах, рассматривающих вопросы производительности в виртуальных окружениях [10;11], основным исследуемым вопросом является определение различий в поведении виртуальной и физической КС. Вопросы, связанные с изменением параметров производительности виртуальной КС при изменении аппаратных ресурсов, выделяемых виртуальной КС, рассмотрены недостаточно глубоко и требуют дополнительного изучения.

К аппаратным ресурсам, которые влияют на производительность КС, относятся следующие:

1. Процессорное время;
2. Оперативная память;
3. Подсистема ввода\вывода (дисковая подсистема).

В различных реализациях систем виртуализации ограничение этих ресурсов для виртуальных КС реализуется по совпадающим подходам. Для ограничения процессорного времени каждой виртуальной КС можно назначить один или несколько процессоров, в зависимости от аппаратной возможности системы, где запущена система виртуализации. Для более гибкого управления выделяемых ресурсов процессорного времени возможно указывать, какую часть рабочего времени процессора может занимать виртуальная КС. Данная возможность позволяет эмулировать изменение рабочей частоты процессора,

что является важнейшим параметром в определении параметров производительности.

Ограничение в использовании оперативной памяти виртуальной КС позволяет задать максимальный объем оперативной памяти, доступный для виртуальной КС.

Ограничение подсистемы ввода\вывода реализуется путём подсчёта операций ввода\вывода, которые производит виртуальная КС. При превышении заданного числа операций за единицу времени последующие запросы на операции ввода\вывода отклоняются. Данная возможность позволяет эмулировать различную скорость работы устройств ввода\вывода.

Таким образом, использование технологии виртуализации позволяет гибко варьировать аппаратные ресурсы, доступные КС. Это предоставляет возможность исследовать параметры производительности виртуальных КС и качество работы сервисов, предоставляемых ими, при различных аппаратных ресурсах этой виртуальной КС. Данный подход позволяет проверить точность аналитических моделей производительности, если они существуют для данного сервиса. В случае отсутствия или невозможности создать аналитическую модель производительности, подход позволяет получить зависимость между параметрами производительности и аппаратными ресурсами в виде таблицы. Табличный вид зависимости позволяет с помощью статистических методов получить статистическую модель производительности КС.

Література

1. Gunther N. J. Analyzing Computer System Performance with Perl::PDQ 2nd Edition / N. J. Gunther. – Verlag Berlin Heidelberg : Springer, 2011 – 422 с.
2. Менаске Д.А., Алмейда В. Ф. Производительность Web-служб. Анализ, оценка и планирование / Д.А.Менаске, В. Ф. Алмейда.; пер.с англ.. – СПб.: «ДиаСофтЮп», 2003. – 480 с.
3. Portnoy M. Virtualization Essentials /Matthew Portnoy.– Indianapolis : Wiley, 2012. – 286 с.
4. Князєва Н. О., Князева О. А. Теорія проектування комп'ютерних систем і мереж./ Н. О. Князєва, О.А. Князєва. – Одеса : ВМВ, 2008. – 212 с.
5. Vmware [Электронный ресурс] – Режим доступа к ресурсу: http://www.vmware.com.
6. XEN [Электронный ресурс] – Режим доступа к ресурсу: http://www.xenproject.org.
7. KVM [Электронный ресурс] – Режим доступа к ресурсу: http://www.linux-kvm.org.
8. VirtualBox [Электронный ресурс] – Режим доступа к ресурсу: http://www.virtualbox.org.
9. Hyper-V [Электронный ресурс] – Режим доступа к ресурсу: https://technet.microsoft.com/en-us/library/mt169373.aspx
10. Application Performance Modeling in a Virtualized Environment / Sajib Kundu, Raju Rangaswami, Kaushik Dutta, Ming Zhao // High Performance Computer Architecture (HPCA), IEEE 16th International Symposium, Bangalore, 2010, 10 с.
11. Resource Allocation in Contending Virtualized Environments through Stochastic Virtual Machine Performance Modeling and Feedback / C. Jiang, X. Xu, J. Zhang, Y. Li, J. Wan // Chinagrid Conference (ChinaGrid), Liaoning , 201 l, 29 с.

УДК 621.391

ЗАБЕЗПЕЧЕННЯ СТРУКТУРНОЇ ЖИВУЧОСТІ СИСТЕМИ НАДАННЯ ІНТЕЛЕКТУАЛЬНИХ ПОСЛУГ

Зіменко Л.М.

Одеська Національна академія харчових технологій
Інститут холоду, кріотехнологій і екоенергетики ім. В.С. Мартинівського
вул Канатна, 112, г. Одеса, Україна, 65039
E-mail: zimenko.liliya@gmail.com

Ensuring Structural Survivability of the System for Providing Intellectual Services

It is considered the issue of ensuring structural survivability of the system to provide intellectual services that is presented as a sequence of elements.

При проектуванні та реалізації мережі наступного покоління існує необхідність забезпечення живучості мережі та окремих її вузлів.

Живучість мережі – здатність мережі зберігати і відновлювати виконання основних функцій в заданому обсязі і протягом заданого часу в разі зміни структури мережі і/або алгоритмів та умов її функціонування внаслідок несприятливих впливів [1].

У зв'язку з тим, що інтелектуальні послуги розвиваються і набули широкого застосування, підтримання живучості системи надання інтелектуальних послуг є актуальним завданням. Інтелектуальна послуга (ІП) – додаткова послуга мережі електрозв'язку, при наданні якої відбувається зміна процесу обслуговування виклику в частині процедур маршрутизації або тарифікації, тобто для цих цілей реалізована спеціальна логіка надання [2]. На рис. 1 представлений приклад надання інтелектуальної послуги.

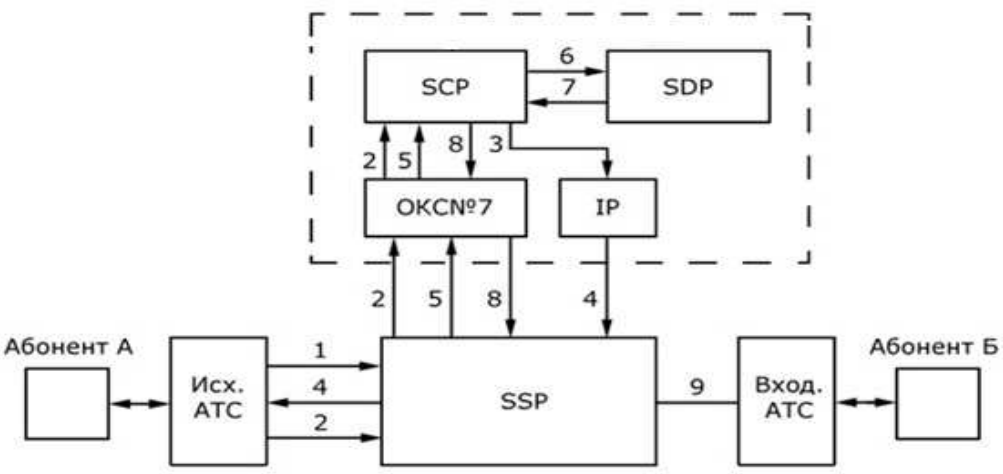


Рис. 1 Алгоритм взаємодії пристроїв при наданні ІП

Схематично ланцюг пристроїв, що працюють при наданні ІП, представлений на рис. 2.

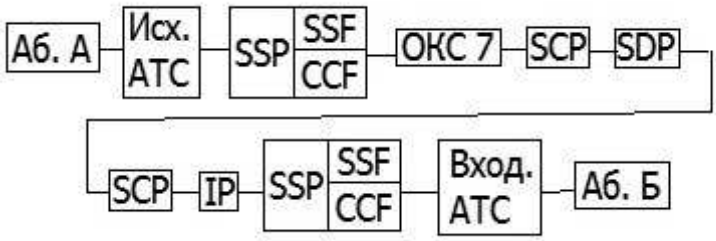


Рис. 2. Схема взаємодії пристроїв під час надання ІП.

Позначення на схемі:

- SSP – вузол комутації послуг (Service Switch Point);
- SCP – вузол управління послугами (Service Control Point);
- IP – інтелектуальний периферійний пристрій (Intellectual Peripheral);
- SDP – вузол бази даних (Service Data Point).

Абонент А набирає номер, програмний комутатор SSP (Softswitch) через сигнальну мережу ОКС-7 призупиняє процес обслуговування телефонного виклику і транслює запит на послугу в SCP. Далі вузол управління послугами звертається до серверу баз даних SDP. Дані, отримані від SDP знову надходять на SCP, SCP передає голосову команду за допомогою голосового інтерфейсу IP абоненту Б через програмний комутатор.

Так як в процесі надання ІП елементи на рис. 2 включаються в роботу послідовно, то живучість (ймовірність неураження системи з n взаємонезалежних елементів) системи надання ІП можна визначити наступним чином:

$$P_{\text{СИС}} = \prod_{i=1}^{n} P_i \,, \tag{1}$$

де $P_{СИС}$ – ймовірність неураження системи надання інтелектуальних послуг;

P_i – ймовірність неураження роботи *i*-го елементу системи;

i – номер елементу в системі.

Як видно з рис. 2, в процесі надання ІП утворюється послідовність елементів, в якій деякі *i*-і елементи системи (наприклад, SCP,SSP) можуть використовуватися кілька разів, наприклад, m_i разів. Тоді ймовірність неураження *i*-го елементу системи виражається як $P_i^{m_i}$. Однак, оскільки вірогідність неуражені таких елементів залежить не від того, скільки разів вони беруть участь в послідовності елементів, а від їх характеристик, згідно із [4, 5] для цих елементів справедлива рівність (2):

$$P_i^{m_i} = P_i^{(1)}, \tag{2}$$

де m_i – кількість входжень *i*-го елементу в системі надання ІП.

При функціонуванні системи надання ІП повинна виконуватися умова (3):

$$P_{\text{СИС}} \geq P_{TP}, \tag{3}$$

де P_{TP} – необхідний показник живучості.

У випадку зовнішнього несприятливого впливу на систему надання ІП при пошкодженні елементів системи, може статися невиконання умови (3). Для забезпечення виконання цієї умови пропонується застосувати структурне резервування окремих елементів системи.

Задача забезпечення структурної живучості системи надання ІП формулюється як пряме завдання оптимального резервування: мінімізувати значення цільової функції (4) при виконанні обмеження (3). В результаті вирішення задачі визначається вектор оптимальної структури резерву $X(x_1, x_2, ..., x_i, ..., x_n)$, кожна координата якого визначає необхідну кількість резервних елементів, які слід підключити до відповідного елементу системи.

$$C_{\text{СИС}} = \prod_{i=1}^{n} c_i x_i \rightarrow \min, \tag{4}$$

де $C_{СИС}$ – вартість системи резервних елементів;

i – номер елементу в системі;

c_i – вартість *i*-го резервного елементу системи;

x_i – кратність резервування *i*-го елементу системи.

Вирішення оптимізаційної задачі – мінімізація функції цілі (4) при обмеженні (3), може бути отримано одним з відомих методів математичного програмування, наприклад, методом градієнта.

В результаті визначення вектору оптимальної структури резерву $X(x_1, x_2, ..., x_i, ..., x_n)$ і підключення відповідної кількості x_i результуючих елементів до кожного *i*-го елементу системи забезпечується необхідне значення P_{TP} структурної живучості системи надання ІП.

Література

1. NGN [Электронный ресурс] // Режим доступа: http://ru.wikipedia.org/wiki/NGN (Дата обращения 10.03.2016).
2. Додонов А.Г. Живучесть информационных систем / А.Г. Додонов, Д.В. Ландэ. – К.: Наук. думка, 2011. – 256 с.
3. ISDN - Интеллектуальные сети. Материал из Национальной библиотеки им. Н. Э. Баумана. [Электронный ресурс] // Режим доступа: http://ru.bmstu.wiki/ISDN_-_Интеллектуальные_услуги (Дата обращения 11.03.2016).
4. Князєва Н.О. Теорія проектування комп'ютерних систем і мереж. Ч.2. Методи аналізу і синтезу комп'ютерних мереж / Н.О. Князєва. Одеса: СПД Бровкін О.В., 2012. -240 с.
5. Давыдов Г.Б. Сети электросвязи / Г.Б. Давыдов, В.Н. Рогинский, А.Я. Толчан. – М.: Связь, 1977. – 360 с.

УДК 621.391

ВПРОВАДЖЕННЯ ХМАРНИХ СЕРВІСНИХ СИСТЕМ В НАЦІОНАЛЬНОМУ МЕРЕЖНОМУ СЕГМЕНТІ УКРАЇНИ

Демидов І.В., Шпур О.М.
Інститут телекомунікацій, радіоелектроніки та електронної техніки
Національний університет «Львівська політехніка», Україна
E-mail: o.shpur@gmail.com, bogdan_str@ukr.net, ivan.demydov@gmail.com

Implementation Cloud Service Systems in the national network segment

In this paper proposed implementation architectural peculiarities of cloud technologies that use existing private cloud structure to support the government service systems at significantly reducing capital expenditures, provided support to the required level of security.

В сучасних соціально-політичних, а також економічних умовах, враховуючи розвиток нових мережних та інформаційних технологій, на перший план виходить проблематика впровадження повсюдного комп'ютингу, що має на меті скорочення споживання обчислювальних ресурсів для розв'язання більш широкого кола задач оброблення інформації в рамках надання необхідних розподілених сервісів [1].

Світовий досвід вказує на те, що хмарні платформи та сервіси дозволяють забезпечити підвищені можливості для швидкого розвитку сервісних застосувань у всіх галузях народного господарства України, в тому числі за рахунок множинного перевикористання сервісних застосувань та їх компонентів різними державними та недержавними організаціями. Спеціалізованими напрямами досліджень у даному контексті їх використання, окрім кібербезпеки, є методи забезпечення гарантованості інформації (Information assurance [2]), яка включає захист цілісності даних, доступність даних та відповідних інформаційних сервісів, аутентифікаційні задачі та конфіденційність даних користувачів. Очевидно, такі методи повинні включати використання фізичних, технічних, а також адміністративних засобів. Важливими питаннями є також забезпечення системної адаптивності [3], неперервності функціонування (належного рівня сервісної доступності), функціональної стійкості, ефективності впровадження сервісів, управління міграцією сервісів та даних, подолання залежності від мереж доступу, що, зокрема, є тактичним завданням сучасних безпровідних технологій доступу.

Для подолання зазначених викликів та розв'язання окреслених задач необхідна синхронізація зусиль операторів телекомунікацій, інфокомунікаційних провайдерів (сервісних операторів), шляхом консолідації їх дата-центрів (ЦОД), а також проектних організацій під егідою державних наглядових органів, які в кінцевому результаті приведуть до вироблення спільної політики ефективного впровадження хмарних технологій, тобто створення відповідної методології відповідно до галузевих чи загально суспільних потреб. Такі заходи дозволять уникнути впровадження непродуктивних обчислювальних та мережних потужностей. Метою даного

дослідження є пошук шляхів оптимальної консолідації для своєчасних трансформацій єдиного національного інформаційного простору України.

Очевидно, що будь-які трансформації у складних системах не є миттєвими. Передача мережної інфраструктури до сфери відповідальності провайдерів інфокомунікацій є ефектним рішенням, яке дозволить загострити увагу персоналу, що відповідає за програмне забезпечення не на експлуатації апаратних засобів, які підтримують та надають обчислювальні потужності, а на створенні сертифікованих програмних продуктів для модифікованого мережного середовища. Хмарне мережне середовище (рис. 1) національного сегменту сервісних мережних систем, за умови дотримання єдиних стандартизованих вимог до впровадження операторського обладнання, є надійною основою для підтримки концепції повсюдного комп'ютингу в різних галузях народного господарства України, а також побудови захищених відомчих інформаційно-телекомунікаційних систем.

Рис. 1. Хмарне середовище національного сервісного мережного сегменту.

Для впровадження хмарних сервісних систем в мережний сегмент нашої держави необхідно:

1. Початкове впровадження хмарних сервісів: визначення державної стратегії, управлінської структури та шляхів ефективного розвитку, аналіз та розширення користувацької бази, сфер застосування (державні та комерційні сервіси, зокрема e-government). Основною трудністю впровадження хмарного середовища на національному рівні є необхідність визначення сфер відповідальності державних органів та відомств, а також ключових осіб, що контролюють процеси впровадження національних сервісних систем, міжвідомчу взаємодію та мають достатній набір повноважень для здійснення професійної діяльності у сфері розроблення та реалізації відповідних нормативних документів.

2. Оптимальна консолідація національних ЦОД на основі стандартизованих програмних платформ та групи дата-центрів ядра хмарного середовища, що спрощує адміністрування національного сегменту системи, дозволяє відповідну віртуалізацію та консолідацію даних і сервісних компонентів застосувань; крім того зменшується площина потенційних втручань у роботу системи, зокрема

різного роду мережних атак. Стратегія впровадження хмарного середовища в національному мережному сегменті передбачає розміщення ключових сервісних компонентів та даних у ЦОД ядра для їх захисту та контролю відповідних інформаційних потоків. Це дозволить не лише зменшити завантаженість надлишкових периферійних обчислювальних ресурсів, а і підвищити коефіцієнт утилізації власне задіяного програмного забезпечення, інтероперабельність програмних платформ за умов постійного моніторингу їх функціонування відділом оперативного системного адміністрування.

3. Впровадження консолідованої національної хмарної мережної інфраструктури: інтеграція багатоператорського середовища в рамках консолідації ЦОД, оптимізація надання розподілених сервісів через створену інфраструктуру в рамках прийнятої політики розподіленого використання сервісних компонентів.

4. Підвищення ефективності надання хмарних сервісів: процес виводу сервісних компонентів на обслуговування до сторонніх операторів, підтримка комерційних сервісів, розширення переліку пропонованих мережних сервісів та обсягів їх надання, контроль з боку наглядових органів (НКРЗІ України).

Зусилля регулюючих органів у сфері впровадження хмарних технологій в Україні повинні бути спрямовані на розв’язання таких основних питань:

- підтримка централізованого управління та функціональної прозорості для всіх хмарних систем національного сегменту сервісної мережної інфраструктури;
- сприяння остаточному перенесенню послуг групи «triple play» на IP платформу;
- впровадження та розширення ідентифікаційних сервісів для користувачів електронних сервісів України.

Необхідним є врахування новітніх інфокомунікаційних технологій, що дозволяють адаптувати системну архітектуру до надання більших обсягів та різновидів послуг у безпечному сегменті національної сервісної мережної інфраструктури, що пов’язане, зокрема, з реалізацією концепції IoT.

Література

1. Demydov I. Concept of the migrating firewall to scalable cloud networks / I. Demydov, O. Lavriv, Z. Kharkhalis, Mohamed Mehdi El Hatri // Сучасні проблеми радіоелектроніки, телекомунікацій, комп'ютерної інженерії TCSET'2016 : матеріали XIII Міжнародної конференції, 23-26 лютого 2016, Львів, Славське, Україна / Міністерство освіти і науки України, Національний університет "Львівська політехніка". - Львів : Видавництво Львівської політехніки, 2016. – С. 643-645.
2. https://en.wikipedia.org/wiki/Information_assurance.
3. Стрихалюк Б. М. Структурний та функціональний синтез гетерогенних сервісно-орієнтованих телекомунікаційних мереж : автореферат дисертації на здобуття наукового ступеня доктора технічних наук : 05.12.02 – телекомунікаційні системи та мережі / Богдан Михайлович Стрихалюк ; Міністерство освіти і науки України, Національний університет "Львівська політехніка". – Львів, 2015. – 40 с.

УДК 621.396

СИСТЕМА МОНІТОРИНГУ ПАКЕТНОЇ ЗАТРИМКИ В ПРОГРАМНО-КОНФІГУРОВАНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Климаш М.М., Селюченко М.О., Панченко О.М.
Інститут телекомунікацій, радіоелектроніки та електронної техніки
Національний університет «Львівська політехніка», Україна
E-mail: mklimash@polynet.lviv.ua, m.seliuchenko@gmail.com, oleksij@gmail.com

System for monitoring packet delay in software-defined telecommunication networks

In this paper, the method to measure packet delay has been developed. This method uses each node as a beacon, thus, does not require additional infrastructure. Monitoring the network is the first step towards a SDN forwarding protocol capable to ensure sufficient QoS for all types of applications and traffic.

На сьогоднішній день парадигма SDN набуває все більшої популярності. Безліч IT організацій і мережевих провайдерів застосовує її, в першу чергу, з метою зниження вартості мережевої інфраструктури та витрат на її утримання, а також забезпечення високого рівня керованості, захищеності та надійності мережі [1]. Основною ідеєю SDN є поділ рівня управління мережею (control plane) і рівня передачі трафіку (forwarding plane).

За рахунок централізації стану мережі на рівні управління, SDN дає мережевим адміністраторам гнучкість в налаштуванні, управлінні, захисту та оптимізації мережевих ресурсів за допомогою динамічних, автоматизованих програм SDN. Крім того, вони можуть написати ці програми самостійно, замість очікування впровадження певної функції в закриті програмні середовища мережі.

Сама система SDN складається з двох компонентів: комутатор з підтримкою протоколу Openflow, і SDN контролер. Openflow комутатор, у свою чергу, складається з трьох частин: (1) Таблиця потоків (Flow Table), яка визначає дії комутатора для кожного потоку, (2) Безпечний Канал (Secure Channel), що забезпечує передачу службової інформації між контролером і комутатором, (3) Протокол Openflow, що надає відкритий і стандартизований метод комунікації комутатора з самим контролером. Таким чином, надається стандартний метод для програмування комутаторів без необхідності настройки кожного комутатора окремо. Комутатор Openflow являє собою простий комутуючий елемент, який пересилає пакети між портами. Самі правила для комутації визначаються безпосередньо віддаленим контролером.

Однією з цілей розробки Openflow є впровадження загальної системи, над якою може працювати будь-який бажаючий. Тому Openflow є платформою, незалежної від вендорів і мов програмування. Openflow також є проектом "open source", тобто доступ до вихідного коду є у всіх бажаючих.

В роботі запропоновано систему моніторингу пакетної затримки з кінця в кінець потоків даних в режимі їх передавання. Основна ідея такого рішення полягає у створенні системи комплексного моніторингу параметрів

функціонування мережі, для визначення основних показників QoS потоків. Використання такої системи в програмно-конфігурованій телекомунікаційній інфраструктурі, дасть змогу забезпечити гарантований рівень якості обслуговування інформаційних послуг з кінця в кінець, шляхом динамічного управління мережевими потоками даних. А також, вибирати оптимальні маршрути передавання даних при виникненні несправностей або погіршення одного із параметрів QoS в комутаторах SDN мережі.

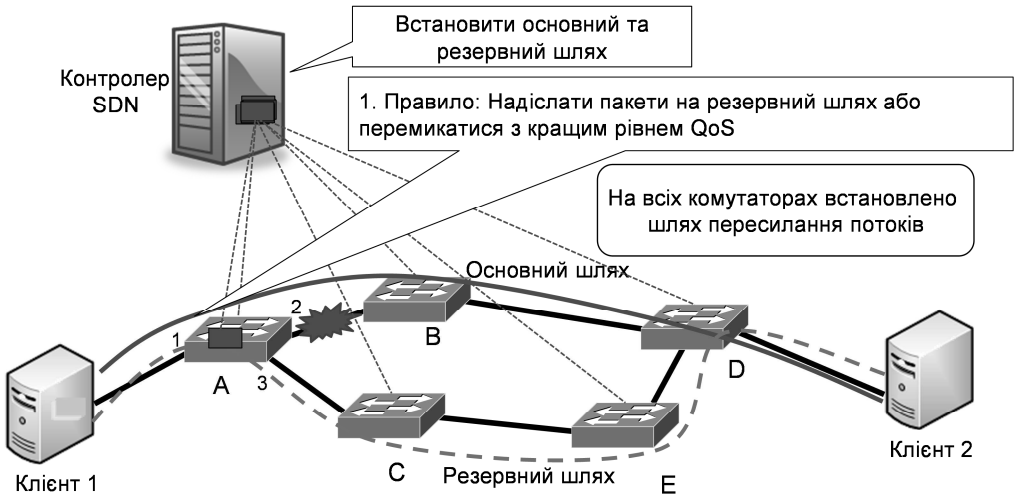


Рис. 1. Принцип функціонування системи моніторингу в SDN мережах.

Реалізація такої системи виконувалась на реальному обладнанні з використанням лінійки комутаторів Openvswitch HP 3500 yl та контролера HP VAN SDN Controller 2.5 встановленого на (Servers: CPU Quad Core 2.6 GHZ, 8 GB RAM, 1 TB hard). Для постановки експерименту використано 2 комутатори та 1 контролер. Розроблена система моніторингу пакетної затримки з кінця в кінець інтегрована на програмно-апаратному комплексі, шляхом добавляння правил комунікації контролера із комутаторами та написанням логіки роботи оцінки затримки потоків при різних навантаженнях каналу на мові Python.

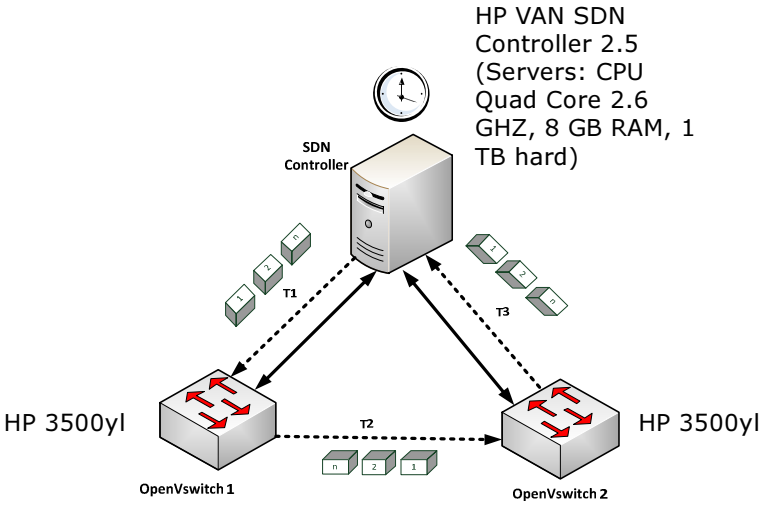


Рис. 2. Експериментальна схема вимірювання затримки потоків з кінця в кінець.

Першим етапом експерименту було моніторинг пакетної затримки при різних навантаженнях на інтерфейс програмного комутатора. Отримані результати отримано на рисунку 3

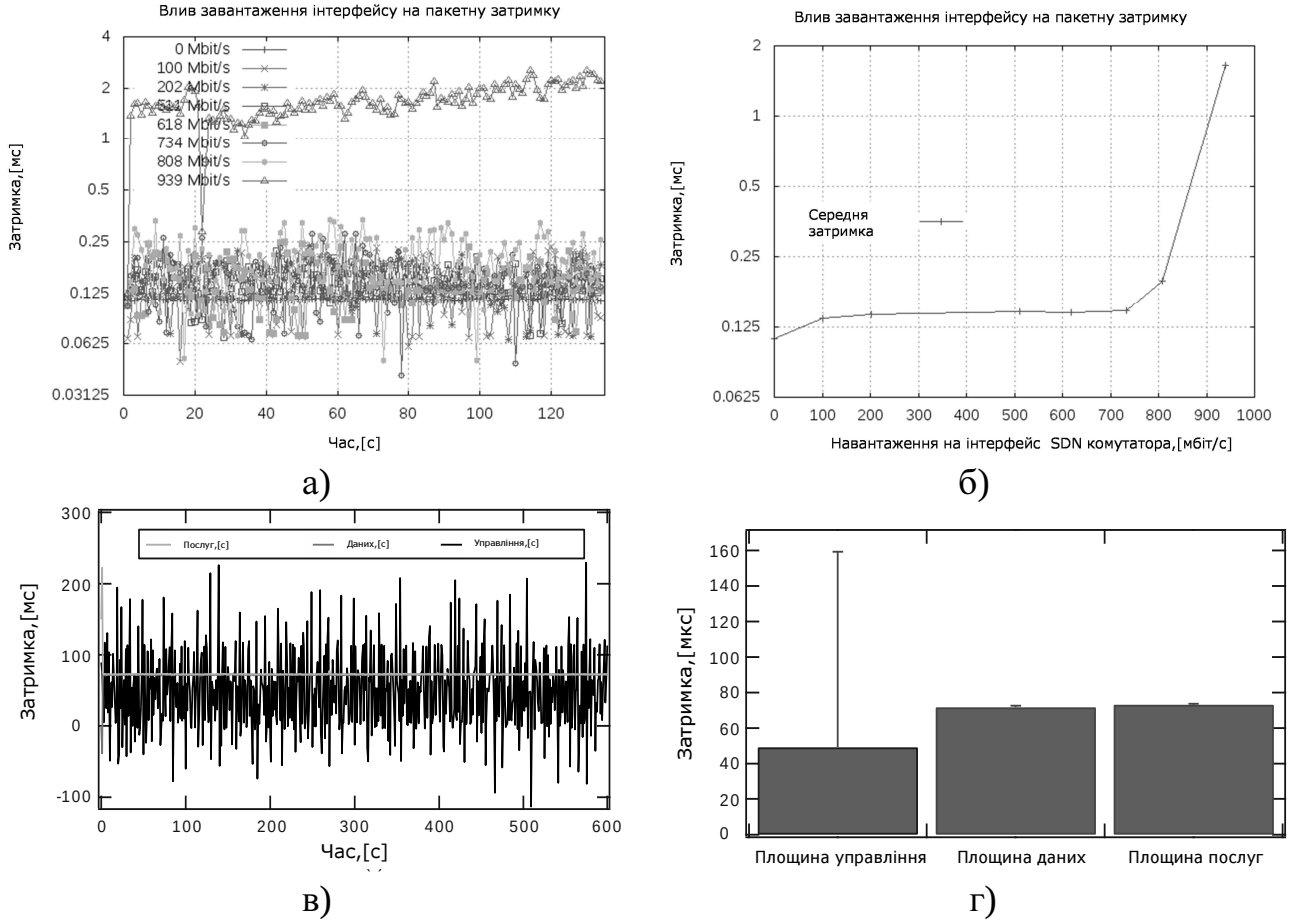


Рис. 3. Результати моніторингу затримки пакетів при різних навантаженнях інтерфейсу а), б) та оцінка затримки на кожній із площині мережі при навантаженні 800 мбіт/с в), г).

Як бачимо при збільшенні навантаження на мережевий пристрій OpenVswitch, пакетна затримка потоку значно зростає при передаванні 939 мбіт/с. Це пояснюється тим, що при максимальному завантаженні інтерфейсу з пропускною здатністю 1Гбіт/с, затримка пакетів зростає за рахунок перевантаження обмеженої таблиці потоків в комутаторах SDN. Трафік потоку генеруються шляхом використання утиліти Iperf.

Висновки. Розроблено систему моніторингу затримки пакетів при передаванні потоків через програмно-конфігуровані вузли. Встановлено, що середня затримка пакетів залежить від завантаження вхідного інтерфейсу і при 100% навантаженні становить 1,8 мс. В умовах незначного навантаження на канал, затримка коливається в межах 128-135 мкс.

Література

1. M. Seliuchenko, M. Beshley, O. Panchenko, M.Klymash, “Development of Monitoring System for End-to-End Packet Delay Measurement in Software-Defined Networks”, Modern problems of radio engineering, telecommunications and computer science Proceedings of the XIII th International Conference TCSET’2016(Lviv – Slavske, February 23–26), 2016. - P. 667-670.

УДК 621.382

МОДЕЛЮВАННЯ DDoS-АТАКИ НА ВЕБ СЕРВЕР

Лаврів О.А., Колодій Р.С., Хархаліс З.М.
Інститут телекомунікацій, радіоелектроніки та електронної техніки, кафедра «Телекомунікації», Національний університет «Львівська політехніка», Україна
E-mail: zenoviy.m.kharkhalis@lpnu.ua

Мосоров В.Я.
Кафедра комп'ютерних наук в економіці, Лодзький університет, Польща
E-mail: wmosorow@uni.lodz.pl

DDoS-attack on a web server modeling

The main reasons DoS-attack is the most popular attack type in the world are listed. Main features of DDoS-attacks are outlined. The real life case modeling of DDoS-attack on web server was performed. Conclusions drawn from the simulation results are presented.

Атаки типу DoS (Denial of Service), чи радше DDoS (Distributed DoS), є одним з основних типів атак на мережеві ресурси на сьогодні. За даними Лабораторії Касперського, на них припадає близько 6% усіх атак 2015 року (порівняно із 4% у 2014) [1].

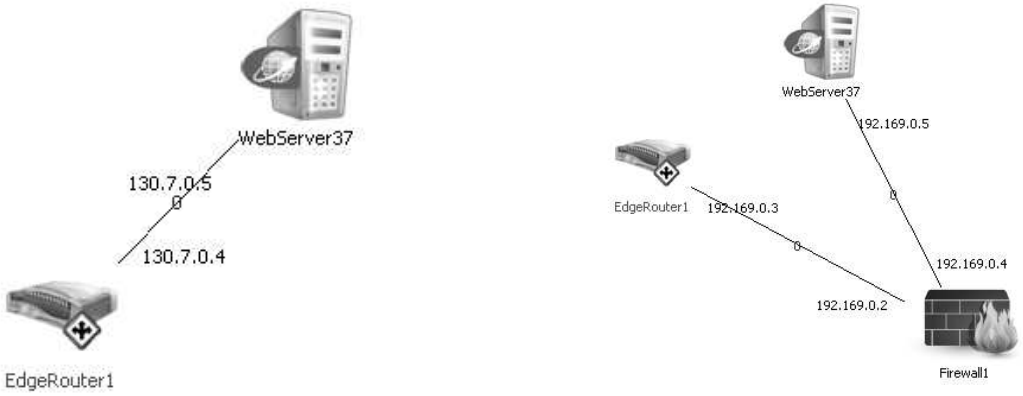
Метою даного дослідження є оцінка ефективності застосування апаратного мережевого екрану для захисту від атак типу DDoS засобами імітаційного моделювання, а також оцінка обсягу необхідних апаратних ресурсів для виконання імітаційного моделювання, яке продемонструє результати, наближені до реальних.

Авторами розглянуто конкретний сценарій DDoS атаки, яка відбулась у 2007 році і була націлена на внутрішню мережу Естонії. Завдяки добре задокументованим фактам [2] вдалось відтворити топологію мережі та провести сплановану DDoS-атаку, параметри і наслідки якої були максимально наближеними до задокументованих.

В загальному випадку, в типовому життєвому циклі атаки виділяють 3 етапи: підготовку, виконання атаки та постфактний період, у якому спостерігаються наслідки проходження атаки. Серед них, етап підготовки є найважливішим та найбільш ресурсозатратним, оскільки вимагає побудови мережі джерел зловмисного трафіку і, що найголовніше, встановлення контролю на цією мережею для синхронного старту атаки і досягнення необхідної для завдання шкоди інтенсивності трафіку. На сьогоднішній день цю проблему вирішують за допомогою т. зв. ботнетів (botnets) [3].

В якості середовища для моделювання вибрано середовище NESSI^2 [4]. Перевагами даної платформи є легкість використання та очевидність представлення в логічному вигляді, де великомасштабні топології можуть мати вигляд однієї іконки. Також було використано можливість платформи автоматично генерувати підмережі із заданими параметрами (напр. за кількістю маршрутизаторів, середньою пропускною здатністю ребер тощо).

Середовище було запущено на відносно слабкій машині з процесором Intel Core Duo T2350 (1.8 МГц), 2 ГБ оперативної пам’яті та ОС Windows Vista.



а) Б)

Рис. 1. Представлені конфігурації: чиста (а) і з мережевим екраном (б).

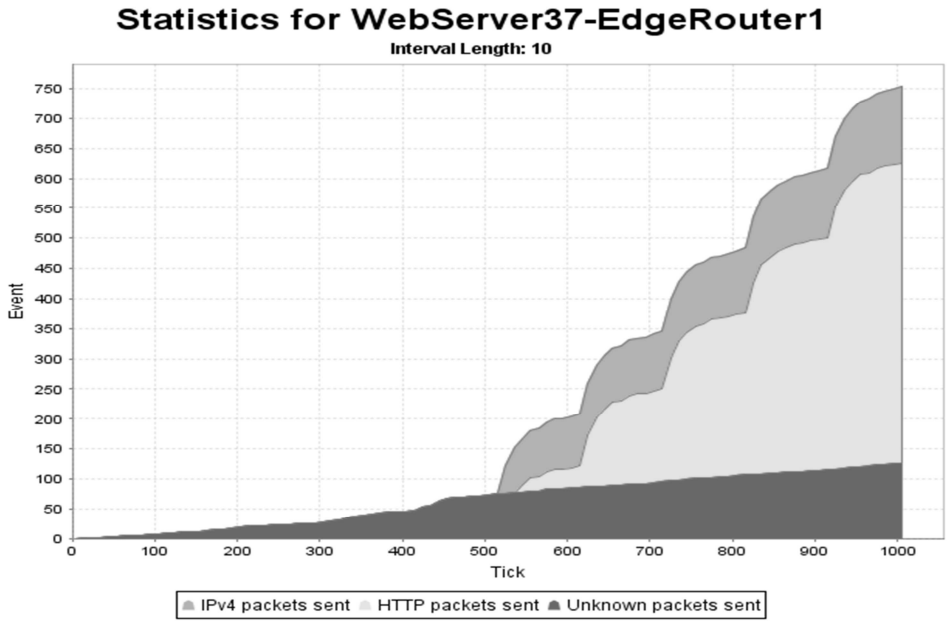


Рис. 2. Атака на веб-сервер без мережевого екрану.

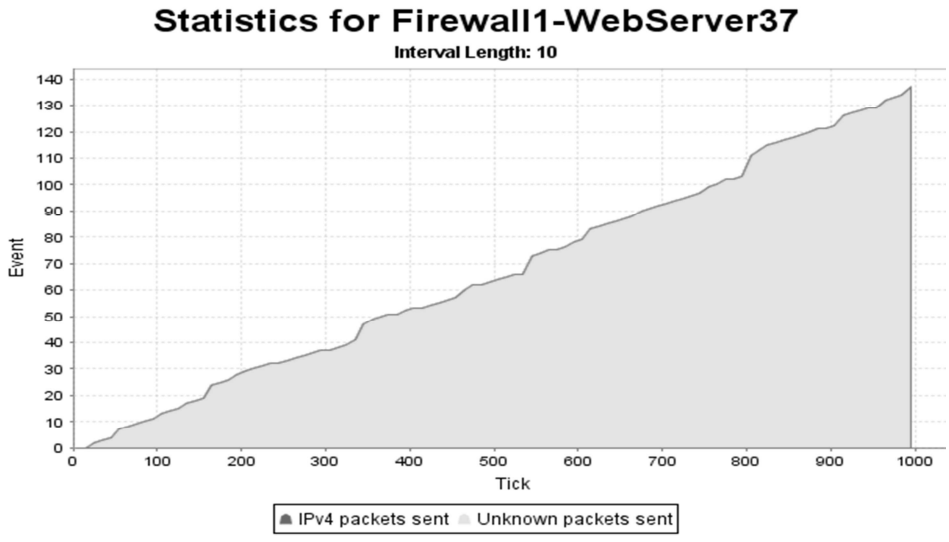


Рис. 3. Атака на веб-сервер з мережевим екраном

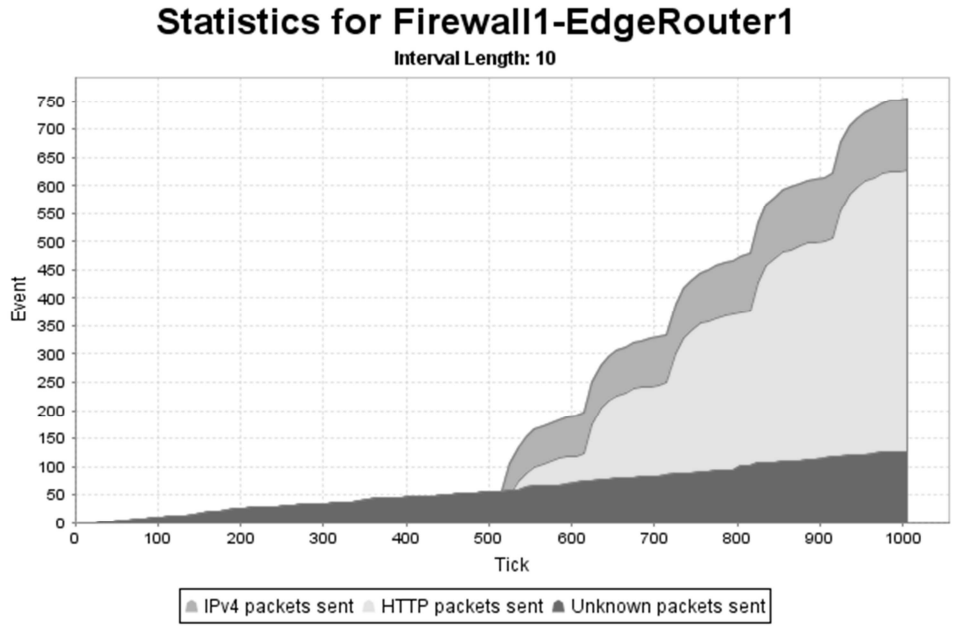


Рис. 4. Внутрішній трафік на мережевому екрані, що захищає веб-сервер

Експериментально визначено, що використовуючи навіть незначні ресурси існує можливість змоделювати доволі масштабну DDoS-атаку, таким чином виділивши слабкі місця у захисті і даючи компетентному персоналу можливість якнайкраще пристосуватись до ймовірних спроб зловмисників завдати шкоди роботі структури.

Порівняно 2 сценарії: змодельовано поведінку трафіку за відсутності та присутності апаратного мережевого екрану між сервером та маршрутизаційною частиною. За наявності мережевого екрану до сервера, що був об'єктом атаки дісталось лише 14% усього шкідливого трафіку, у порівнянні з випадком без екрану (перевантаження у 500%).

Література

1. Юрій Ільїн, Головний редактор Kaspersky Business, Звіт *"IT SECURITY RISKS SPECIAL REPORT SERIES"*, [он-лайн]: https://cdn.press.kaspersky.com/ files/2015/09/ IT_Risks_Survey_Report_Threat_of_DDoS_Attacks.pdf.
2. Merike Kaeo, *"Designing Network Security"*, Cisco Press, oct 30, 2003; [он-лайн]: http:// www.ciscopress.com/store/designing-network-security-9781587051173.
3. Визначення зі словника, [он-лайн]: http://www.dictionary.com/browse/botnet (доступ, травень 2015).
4. Karsten Bsufka and Rainer Bye, *NeSSi² Ver. 2.0.0-beta.3 Manual*, [он-лайн]: http://es.osdn.jp/projects/sfnet_nessi2/downloads/nessi2/2.1.1-beta/NeSSi2Manual. pdf/ (доступ, травень 2015).i

УДК 621.3

ПРИМЕНЕНИЕ КОНЦЕПЦИИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ К ПОСТРОЕНИЮ МОБИЛЬНЫХ СЕТЕЙ НА ОСНОВЕ IP MULTIMEDIA SUBSYSTEM

Слепец Ю.Ю., Гаттуров В.К.
Институт телекоммуникационных систем НТУУ «КПИ», Украина
E-mail: yuriy.slipets@gmail.com

Usege of cloud computing concepts to build mobile networks based on the IP Multimedia Subsystem

This article shows the way of IMS evolution from 2.5G to 4G networks. And as a result comes to cloud solution and becomes the new model of cloud realization for telecommunication networks as IMS as a Service.

В настоящее время операторы сетей мобильной связи сталкиваются с тенденцией снижения темпов роста доходов, получаемых в результате предоставления услуг мобильной связи. Снижение доходов связано со снижением темпов роста абонентской базы операторов, так как рынок услуг мобильной связи постепенно переходит в состояние насыщения, то есть дальнейшее привлечение абонентов возможно только за счет перехода абонентов от одного оператора к другому, но не за счет подключения новых абонентов.

Одним из выходов из сложившейся ситуации считается переход к сетям на основе IP Multimedia Subsystem (IMS). Новая технология доступа 3G сети заранее спроектирована для предоставления услуг, связанных с передачей больших объемов информации, а ее горизонтальная архитектура подразумевает использование общих элементов для предоставления услуг, что не ведет к заметному усложнению сети оператора, как это происходит в случае использования вертикальной архитектуры.

Кроме того, IMS архитектура проектировалась как независимая от технологии сети доступа, что позволяет получать доступ к IMS услугам с любого терминала по любой подходящей технологии доступа (W-CDMA, WiMax, GSM, LTE, LTE Advanced). [1, 2]

Революционным решением переноса огромных объемов денежных затрат на «физическое» построение сетей и внедрение в них дополнительных услуг, стало создание концепции «Облачных вычислений». Данная концепция позволяет создавать фактически весь «интеллект» сети на удаленном вычислительном ресурсе. Также, использование «облака» позволяет гибко реагировать на изменения вычислительных потребностей, используя свойства вычислительной эластичности облачных услуг.

В концепции облачных вычислений выделяют 3 основных модели предоставления услуг:

- **Инфраструктура как сервис (IaaS)** - это модель предоставления компьютерной инфраструктуры как услуги на основе концепции облачных вичислений. IaaS основана на технологии виртуализации, позволяющей

пользователю оборудования делить его на части, которые соответствуют текущим потребностям бизнеса, тем самым увеличивая эффективность использования имеющихся вычислительных мощностей. Пользователь (компания или разработчик ПО) должен будет оплачивать всего лишь реально необходимые ему для работы серверное время, дисковое пространство, сетевую пропускную способность и другие ресурсы. Кроме того, IaaS предоставляет в распоряжение клиента весь набор функций управления в одной интегрированной платформе.;

- **Платформа как сервис (PaaS)** - это модель предоставления интегрированной платформы для разработки, тестирования, развертывания и поддержки веб-приложений как услуги. В этой модели вся информационно-технологическая инфраструктура, включая вычислительные сети, серверы, системы хранения, целиком управляется провайдером, провайдером же определяется набор доступных для потребителей видов платформ и набор управляемых параметров платформ, а потребителю предоставляется возможность использовать платформы, создавать их виртуальные экземпляры, устанавливать, разрабатывать, тестировать, эксплуатировать на них прикладное программное обеспечение, при этом динамически изменяя количество потребляемых вычислительных ресурсов;
- **Программное обеспечение как сервис (SaaS)** – это модель развертывания приложения, которая подразумевает предоставление приложения конечному пользователю как услуги по требованию. Доступ к такому приложению осуществляется посредством сети, а чаще всего посредством Интернет-браузера. В данном случае, основное преимущество модели SaaS для клиента состоит в отсутствии затрат, связанных с установкой, обновлением и поддержкой работоспособности оборудования и программного обеспечения, работающего на нём. Целевая аудитория - конечные потребители. [4]

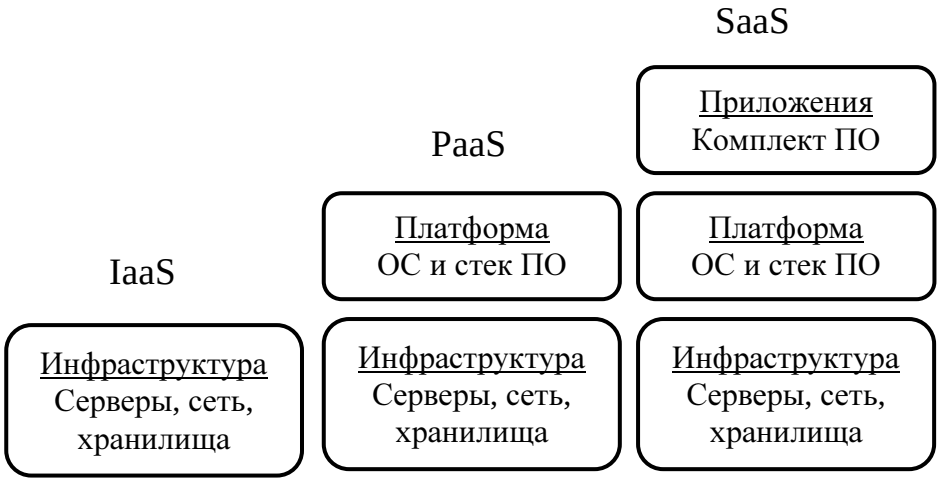


Рис. 1 Иллюстрация к пояснению моделей облачных вычислений.

Исходя из выше изложенного видно, что для построения любых сетей связи (корпоративной сети, мобильной сети масштаба страны, всемирного веб-ресурса) наиболее приемлемыми является модель PaaS, что в то же время накладывает определенные обязательства и ограничения.

Так как IMS была разработана как сервисная платформа для сетей третьего поколения, то свое эволюционное существование в сетях четвертого поколения она займет как реализация облачной сервисной надстройки на сети для реализации концепции 4Play (голос, видео, данные, мобильность). [2]

В случае облачной реализации IMS будет происходить слияние основного функционала (P-CSCF, S- CSCF, I-CSCF, и HSS) в один облачный ресурс. Интеллект каждой из функций реализован на отдельной виртуальной машине (IMS-VM). [1, 3]. Реализация IMS в облаке будет использовать SaaS, так как только в случае отказа от аппаратной реализации, возможна новая эволюционная стадия развития IMS.

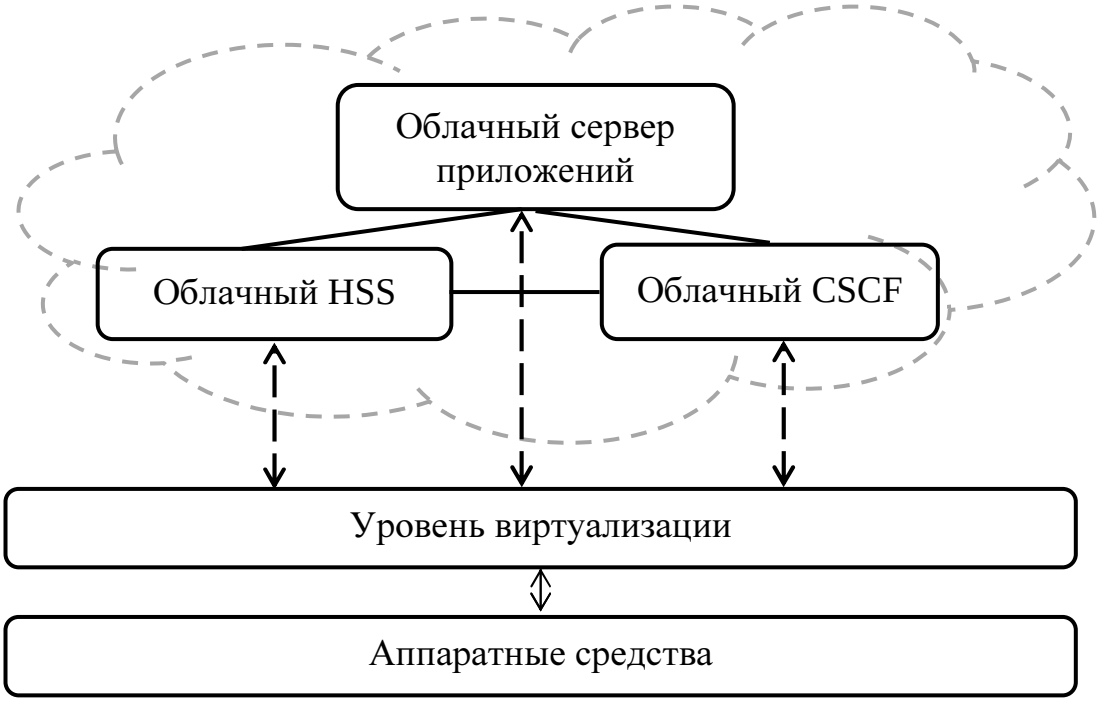


Рис 2. Иллюстрация виртуализации IMS [3]

Вывод. Вследствие эволюции концепции IMS от сетей третьего поколения до четвертого становиться понятно, что для реализации облачного решения IMS наиболее подходящей является SaaS бизнес-модель. В итоге, возникает новое понятие **IMS as a Service**. То есть, весь функционал данной концепции реализован в виде облака и, как следствие, программной надстройки на любой сети четвертого поколения.

Литература

1. Гольдштейн А. Б., Гольдштейн Б. С., SoftSwitch СПб.: БХВ – Санкт-Петербург, 2006. – 368 с.: ил.
2. Бакланов, И. Г. NGN: принципы построения и организации / под ред. Ю. Н. Чернышова. – М.: Эко-Трендз, 2008. – 400 с.: илл.
3. Cloudifying the 3GPP IP Multimedia Subsystem for 4G and Beyond: A Survey Mohammad Abu-Lebdeh, Jagruti Sahoo, Roch Glitho, Constant Wette Tchouati, Concordia University, Montreal, QC, Canada. 8 p.
4. Cloud Computing. Implementation, Management, and Security. John W. Rittinghouse, James F. Ransome. 340 p.

УДК 621.3

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ НАДСТРОЙКИ IP MULTIMEDIA SUBSYTEM AS A SERVICE С ПОМОЩЬЮ STAGED-EVENT DRIVEN ARCHITECTURE

Слепец Ю.Ю., Гаттуров В.К.
Институт телекоммуникационных систем НТУУ «КПИ», Украина
E-mail: yuriy.slipets@gmail.com

Software implementation of IP Multimedia Subsystem as a Service setup by Staged-event driven architecture

This article shows the one of many ways for IP Multimedia Subsystem (IMS) cloud implementation using the Staged-event driven architecture (SEDA) using it's advantages for creating big data services.

На данном этапе развития сетей связи концепция IMS не пользуется большой популярностью. Причиной тому, на момент создания спецификаций 3GPP были следующие факторы:

- Необходимость поддержки протокола IPv6;
- Отсутствие терминалов IMS;
- Необходимость модернизации систем Operation Support System (OSS) и Business Support System (BSS);
- Отсутствие поддержки не SIP-приложений.

Устранение каждой из этих проблем влекло за собой огромные затраты на реорганизацию уже построенных GSM и UMTS сетей. Но в процессе эволюции мира телекоммуникаций и широкое внедрение интеллектуальных технологий, дало возможность преобразовать автономное физическое IMS решение в программную надстройку на уже существующей сети, используя концепцию облачных вычислений. Так совсем недавно появилась еще одна разновидность облачных бизнес-моделей построения дополнительных сервисов - IP Multimedia Subsystem as a Service (IMSaaS).

В случае облачной реализации IMS будет происходить слияние основного функционала (P-CSCF, S- CSCF, I-CSCF, и HSS) (рис 1.) в один облачный ресурс. Интеллект каждой из функций реализован на отдельной виртуальной машине IMS-Virtual Machine (IMS-VM). [1, 3]

Основная проблема модели IMSaaS заключается в создании взаимодействий между функциональными объектами сети, которые будут соответствовать, стандартизированным в 3GPP, интерфейсам взаимодействия.

Предложенный способ реализации облачных функциональных объектов и взаимодействий между ними основан на использовании Staged-event driven architecture (SEDA) – архитектуры для программной реализации систем массового обслуживания.

В этой модели, каждый этап воплощает в себе надежный, многократно используемый программный компонент, который выполняет подмножество обработок запросов. Выполняя контроль допуска для каждой очереди событий (вызовов/заявок), услуга может быть подготовлена для сильной загрузки, предотвращая перегрузку ресурсов, когда превышается выделенный на службу ресурс. [2]

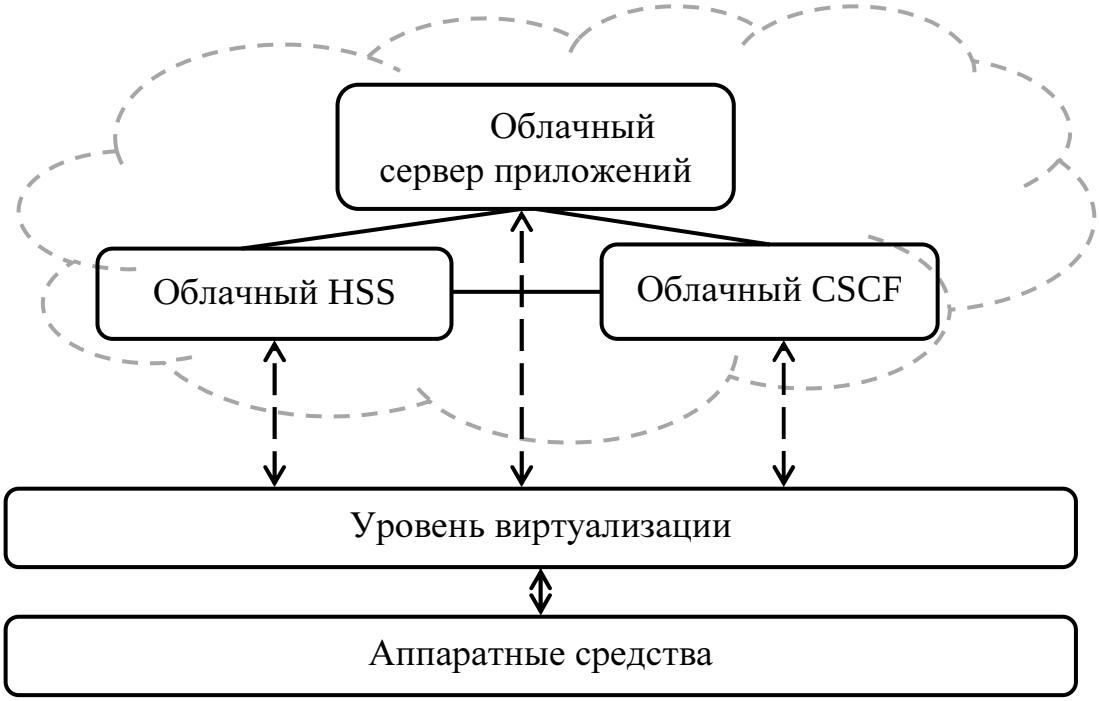


Рис. 1 Иллюстрация упрощенной IMSaaS [3].

SEDA использует динамическое управление временными параметрами (например, параметрами планирования каждого этапа) для управления нагрузкой, например, путем адаптивного сброса нагрузки.

Основной единицей обработки в SEDA является ступень. Ступень представляет собой автономный компонент приложения, который состоит из обработчика событий (event handler), входящей очереди событий (event queue), и пула потоков (thread pool), как показано на рис 2. Каждый каскад управляется одним или несколькими контроллерами, которые влияют на занятие ресурсов, планирование, распределение потоков, и управление доступом. Работа потоков в ступени заключается в извлечении набора событий из входящей очереди и вызове соответствующего обработчика событий. Обработчик событий обрабатывает каждый пакет событий, и отправляет избыточные события/заявки в очереди других ступеней. [2]

Событие обрабатываемое на ступени, как правило, представляет собой запрос клиента интернет-службы, например, запрос HTTP для веб-страницы. Однако события могут представлять другую информацию, имеющую отношение к работе службы, такие как установление сетевого соединения, то есть передачу управляющей сигнальной информации. Программная модель

SEDA использует пакеты событий, так как это позволяет повысить производительность.

Обработчик событий – функция, которая принимает пакет событий в качестве входных данных, обрабатывает эти события, и при перегрузке переводит в очередь других ступеней.

Потоки являются тем самым ключевым процессом реализации «параллелизма» в SEDA. Они выполняют функцию «подхвата» избыточных ступеней других ступеней либо вывода избыточных заявок из своей очереди. [2].

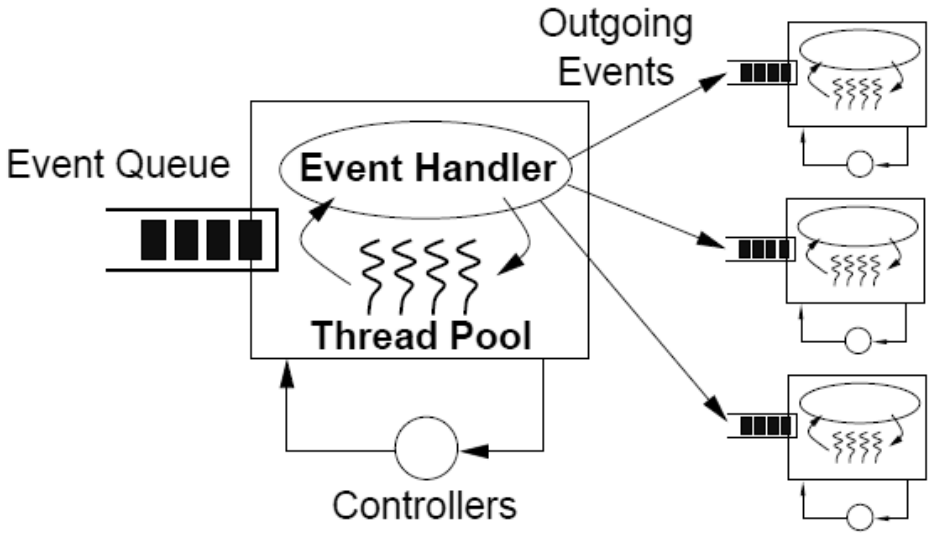


Рис. 2 Ступень SEDA [2].

Преимущество такого подхода заключается в том, что управление продолжением может выполняться приложением, когда это наиболее удобно (т.е. на этапе пересечение границ ступеней), а не в любое время во время операции обработчика событий.

Выводы: SEDA дает возможность создавать программные продукты, которые могут работать с огромным количеством входящих заявок, что является одним из основных признаков телекоммуникационной сети. Соответственно данная архитектура полностью удовлетворяет требованиям для реализации IMSaaS, что будет подтверждено и реализовано в последующей исследовательской работе.

Литература

1. Гольдштейн А. Б., Гольдштейн Б. С., SoftSwitch СПб.: БХВ – Санкт-Петербург, 2006. – 368 с.: ил.
2. An Architecture for Highly Concurrent,Well-Conditioned Internet Services: Matthew David Welsh. 211 p.
3. Cloudifying the 3GPP IP Multimedia Subsystem for 4G and Beyond: A Survey Mohammad Abu-Lebdeh, Jagruti Sahoo, Roch Glitho, Constant Wette Tchouati, Concordia University, Montreal, QC, Canada. 8 p.

УДК 519.17

МЕТОД РОЗПОДІЛЕННЯ ІЄРАРХІЧНОГО МЕТАГРАФА НА РІВНІ

Кривенко А. С., Штогріна О. С., Терновой М. Ю.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: alexakryvenko@gmail.com, L_Shtogrina@mail.ru, ternovoy@its.kpi.ua

Layer assignment method for hierarchical metagraph

This paper describes the method of automatic layer assignment for hierarhical metagraphs. The method walks through paths in metagraph and numerates nodes layers. Metavertices and inner vertices are always assigns to the same layer. Layer assignment method can be used as first step for metagraph visualization method.

На сьогоднішній день метаграфи використовуються для моделювання бізнес-процесів з використанням діаграм виконання робіт, систем підтримки та прийняття рішень, баз нечітких знань, для представлення основних зв'язків даних та логічних правил [1]. При моделюванні процесів часто виявляється, що отримувана модель має залежності входів одних елементів від виходів інших та не має циклів, що свідчить про присутність у моделі ієрархічності. Оцінити та проаналізувати такі моделі можна за допомогою їх візуального представлення. Візуалізація ієрархії це один із способів оцінити відносини в ієрархічній моделі, кількість рівнів і кількість вузлів на рівні.

Введемо поняття ієрархічного метаграфа, як метаграфа, що має корінь – вузол, який є початком всіх простих шляхів у метаграфі.

Зазначимо, що простий шлях в орієнтованому метаграфі S від вузла mv_p в вузол mv_q – це послідовність дуг $Path(mv_p, mv_q) = (e_1, e_2, ..., e_n)$, така що $\forall i : mv_i^{in} \cap mv_{i+1}^{out} \neq \varnothing$. Довжина шляху у метаграфі це кількість ребер у послідовності $\{e_n\}$ [2].

Існує велика кількість алгоритмів, які дозволяють візуалізувати ієрархічні графи. Це силові алгоритми та алгоритми на основі Sugiyama framework, що є набором правил естетичності для зображення ієрархічного графа:

- ребра повинні бути однаково напрямлені;
- короткі ребра краще сприймаються;
- вузли мають бути рівномірно розподіленими;
- перетин ребер ускладнює сприйняття;
- прямі ребра краще сприймаються.

Застосування стандартних силових алгоритмів [3-6] для ієрархічних графів не дозволяє отримувати зображення, на яких можна переглядати рівні ієрархії окремо одне від одного і швидко оцінювати взаємозв'язки між рівнями ієрархії. Наприклад, у роботі [3] граф моделюється як система кульок пов'язаних пружинами, що можуть притягати та відштовхувати їх. У результаті координати вузлів на площині переважно рівномірно розподілені та напрям ребер не враховується. Описаний в роботі [4] алгоритм зображує вузли з більшою

кількістю вхідних та вихідних ребер ближче до центра площини за рахунок сили гравітації. Сугіяма та Мізю представили силовий алгоритм, де додано силу магнітного поля, яка спрямовує ребра у його напрямку [5].

На основі Sugiyama framework були представлені алгоритми розділення графів на рівні [7], що одразу визначають позиції вузлів після призначення їм рівня. Основною їх перевагою перед силовими алгоритмами є те, що отримані зображення цілком очікувані, та вузли завжди мають фіксовані позиції. Завдяки цьому результати завжди придатні для подальшої оптимізації, яка може включати додання «пустих» вузлів, зменшення перетинів ребер, накладення умов на довжину і ширину ієрархії.

Для візуалізації ієрархічних метаграфів необхідно насамперед розподілити всі вузли по рівням. Будемо вважати метаграфом розділеним на рівні метаграф, кожна вершина якого відповідає деякому рівню, причому всі вкладені у метавершину вершини належать тому самому рівню, що і метавершина. Таким чином, метавершина може знаходитись тільки на одному рівні. Номер рівня має відповідати довжині простого шляху від кореня до вузла метаграфа.

Так як метаграф є структурою, яка допускає вкладеність вузлів, виникає проблема визначення рівнів, до яких відносяться вузли метаграфа. Завдання візуалізації ієрархічного метаграфа вимагає врахування більшої кількості обмежень, ніж при знаходженні графічного зображення графа. Це є результатом того, що метавершини можуть перетинатися так, що визначення позицій вузлів у границях рівня буде досить складною задачею. Саме тому для зображення вузлів ієрархічного метаграфа у границях рівня найкраще підходять силові алгоритми. Враховуючи вимогу до того, щоб кожен рівень був візуально окресленим пропонується двоступеневий метод візуалізації. На першому етапі вузлам призначаються мітки рівня за допомогою методу розділення метаграфа на рівні, а на другому етапі відбувається візуалізація за допомогою силового методу.

Представлений раніше [8] метод візуалізації метаграфів може бути модифікований для того щоб візуалізувати ієрархічні метаграфи. Рекомендації до візуалізаці ієрархічного метаграфа силовим методом були надані у роботі [9]. Даний метод візуалізації ієрархічних метаграфів потребує щоб вузли метаграфа були впорядковані по рівнях перед початком візуалазації, чого не було розглянуто у роботі.

Впорядкування вузлів по рівнях пропонується зробити за наступним алгоритмом, що є модифікацією алгоритму найдовшого шляху представленого у роботі [7]. Спочатку визначається найдовший шлях у ациклічному метаграфі, його довжина дорівнює K. Далі вузлам, які не мають вихідних ребер призначають пріоритет K. Якщо всі безпосередні наступники вузла вже мають призначений пріоритет цьому вузлу призначається найнижчий пріоритет з його безпосередніх наступників мінус один. Це повторюється до тих пір доки всім вузлам не буде призначений пріоритет. Вузли з однаковим пріоритетом формують рівень ієрархії.

Щоб обчислити множину безпосередніх наступників для вузла mv у метаграфі візьмемо усі ребра, які виходять з вузла mv, або з метавершини, яка включає mv. Усі кінцеві вузли, та метавершини, що їх включають і будуть

безпосередніми настуниками вузла *mv*.

У запопонованому алгоритмі використовується дві множини метавершин *H* і *Z*, які є порожніми на початку. Значення змінної поточного рівня є міткою рівня, який в даний час будується. Як тільки метавершина отримує мітку рівня вона також додається до множини *H*, та всім її вкладеним вершинам також призначається той самий рівень. Таким чином, *H* є множиною всіх метавершин, для яких вже визначений рівень. Множина *Z* є множиною всіх вузлів, що належать рівню нижче поточного рівня.

На кожній ітерації алгоритму обирається метавершина *mv*, якій буде присвоєна мітка рівня. Вона обирається серед метавершин, для яких не був визначений рівень, тобто $mv \in M \setminus H$, де *M* – множина всіх метавершин, і для яких всі їх безпосередні наступники належать рівню нижче поточного, тобто лежать у *Z*. Якщо жодної метавершини не було обрано, то побудова рівня закінчена, мітка рівня збільшується на одиницю та до множини *Z* додаються всі метавершини з *H*. Алгоритм зупиняється, коли множини *H* та *M* однакові.

Перевагами цього алгоритму є його простота та лінійна складність. При візуалізації ієрархія має висоту, що дорівнює довжині найдовшого шляху у метаграфі. Через це у більшості випадків кількість метавершин на нижніх рівнях збільшується.

Запропонований метод розділення метаграфа на рівні може бути застосований для отримання графічного зображення ієрархічних ациклічних метаграфів. Планується доопрацювання методу з метою додати фазу, на якій будуть прибрані всі цикли у метаграфі.

Литература

1. Терновой М.Ю., Штогріна О.С. Представлення баз нечітких знань за допомогою метаграфа та проведення нечіткого логічного виведення на його основі // Вісник Харк. нац. ун-ту., Сер. «Математичне моделювання. Інформаційні технології. Автоматизовані системи управління», № 1105, 2014. –С. 156 – 165.
2. Basu A. Metagraphs and their applications / A. Basu, R. W. Blanning, // Springer – 2010. – 173p.
3. Fruchterman T. M. J. Graph Drawing by Force-Directed Placement / T. M. J. Fruchterman, E. M. Reingold // Software-Practice and Experience. – 1991. – Vol. 21. – No.11. – P. 1129-1164.
4. Frick A. A Fast Adaptive Layout Algorithm for Undirected Graphs / A. Frick, A. Ludwig, H. Mehldau // Springer-Verlag. – 1995. – Vol. 894 – P. 388-403.
5. Sugiyama K. A Simple and Unified Method for Drawing Graphs: Magnetic-Spring Algorithm / K. Sugiyama, K. Misue // Proceedings of Graph Drawing: Conf., 1994, New Jersey: proc. of conf. / Springer-Verlag.– 1995. – Vol. 894 – P. 364–375.
6. Kamada T. An algorithm for drawing general undirected graphs / T. Kamada, S. Kawai // Information Processing Letters. – 1989. – V. 31. – P. 7-15.
7. Patrick Healy and Nikolov S. Nikolov. Handbook of Graph Drawing and Visualization, chapter II.16. Hierarchical Drawing Algorithms / CRC Press – 2013. – P. 409-446.
8. Штогрина Е. С., Кривенко А. С. Метод визуализации метаграфа // Научно-технический вестник информационных технологий, механики и оптики. – 2014. – № 3 (91). – С. 124–130.
9. Кривенко А.С., Штогрина Е.С. Визуализация иерархических метаграфов // Проблеми телекомунікацій : 9-а Міжнар. наук.-техн. конф., 21-24 квіт. 2015р. : матеріали конф. – К., 2015. – С. 310–313.

УДК 004:931

МЕТОДИ РОЗПІЗНАВАННЯ ТЕКСТУ

Репік С. І., Штогріна О. С.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: sergrepik@gmail.com, l.shtogrina@gmail.com

Methods of text recognition

This paper presents handwriting recognition method that is based on the methods of comparison with etalon. In this method the step on which sample symbols is comparing with etalons was modified. When there is a letters comparison it used their center of mass. Contributed modification increases the recognition rate. This is possible by reducing the number of operations of overlay letters on etalon, when they compares.

Підчас повсякденної діяльності державні структури, бізнес, наукові та навчальні організації використовують велику кількість паперових документів, більшість з яких є рукописними. Велика кількість даних та знань міститься в друкованих або рукописних документах, які є архівними. Зростає потреба в оцифруванні паперових документів, з метою подальшої обробки їх вмісту автоматизованими комп'ютерними системами.

Розпізнавання тексту можна розділити на кілька напрямів, які досить суттєво відрізняються методами їх вирішення. Текст може бути друкований чи рукописний. Будь який з них може бути додатково структурований. Наприклад, формули можуть містити різні рівні записів, такі як надстрочні, підстрочні, спеціальні позначки математичних дій, тощо.

На сьогоднішній день існує ряд методів, що вирішують проблему розпізнавання друкованого тексту, однак досі не існує систем, здатних розпізнавати будь-який рукописний текст [1]. Існуючі системи можуть досить не якісно розпізнавати конкретні почерки. Отже актуальною є задача розробки методу розпізнавання рукописного тексту, який дозволить опрацьовувати рукописні документи.

Перед тим як відбувається розпізнавання тексту, завжди існує попередня обробка вхідного зображення. Першим її етапом є покращення якості зображення. На цьому етапі підвищують контрастність та різкість зображення, а також здійснюється фільтрація від шумів. Наступним етапом є сегментація [2], за допомогою якої визначається структура тексту. Сегментація дещо відрізняється для друкованого та рукописного тексту. В обох випадках виділяються строки, слова та літери, але для друкованого тексту сегментація літер набагато простіша та відбувається подібно до сегментації слів – за допомогою методу горизонтальних та вертикальних профілів [3]. Для рукописного тексту сегментація на рівні літер складніша: літери можуть зливатися у один сегмент або навпаки, одна літера розпадатися на кілька сегментів. Це суттєво ускладнює задачу розпізнавання.

Після попередньої підготовки, методи розпізнавання рукописного і друкованого тексту відрізняються більш суттєво. Для друкованого тексту

застосовується порівняння сегментованих літер з еталонами із різноманітних шрифтів. Знайшовши співпадіння з одним із них, наприклад, першої літери, залишок тексту, циклічно розпізнається за рахунок порівняння усіх виділених сегментів з літерами визначеного шрифту.

Для рукописного тексту порівняння з еталонами шрифтів принципово не можливе – кожен почерк є унікальним, отже еталону, на зразок шрифту, не існує. Спочатку необхідно створити базу еталонів конкретного почерку, з якою надалі відбуватиметься порівняння.

Існує два підходи до розпізнавання рукописного тексту – розпізнавання онлайн та офлайн [4]. Перший передбачає розпізнавання безпосередньо підчас написання тексту і використовує алгоритми написання символів, котрі враховують траєкторію руху «пера» – предмету, яким здійснюється написання. Цей підхід називають розпізнаванням онлайн. На сьогоднішній день, задачу такого розпізнавання для більшості мов можна вважати вирішеною. Сучасні електронні записники широко його використовують. Другий підхід має на меті розпізнавання рукописного тексту, який було написано заздалегідь. Розпізнавання офлайн набагато важливіше, так як кількість вже написаного тексту величезна. Проблема саме такого розпізнавання у загальному випадку досі не вирішена.

Існує два основні типи методів вирішення задачі розпізнавання тексту офлайн – структурні та еталоні, а також їх комбінації [4].

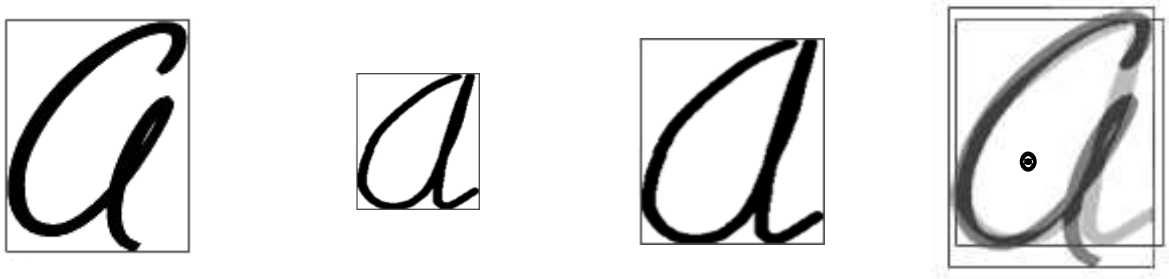
Структурні методи засновані на виділенні та аналізі різних структурних елементів символу, їх ознак та властивостей. Кожна літера розбивається на вузли та криві, що їх з’єднують. На основі набору таких даних робиться висновок, яка літера написана. Однак існує проблема, пов’язана із тим, що більшість літер написані не каліграфічно та, відповідно не мають чітких з’єднань.

Еталоні методи передбачають порівняння заданого, не розпізнаного символу з набором деяких еталонів. Для цього використовують нейронні мережі, які необхідно заздалегідь заповнити еталонами. Існують кілька алгоритмів порівняння тексту з еталоном. Найпростіший варіант – попіксельне порівняння, однак для нього необхідні рівні по розмірам зображення, що порівнюються. Інші варіанти – накладення та накладення зі зміщенням, у яких зображення ставляться у відповідність одне одному. Методи еталонного порівняння рукописного та друкованого тексту, на перший погляд, схожі, однак суттєво відрізняється. Еталони рукописного тексту, на відміну від літер шрифту, лише грубі зразки. Це значно збільшує вірогідність помилки.

В роботі запропоновано метод розпізнавання рукописного тексту, що базується на методах еталонного порівняння, в якому модифіковано етап порівняння зразку літер з еталоном таким чином, що при співставленні літер враховуються їх центри мас. Внесена модифікація дозволяє збільшити швидкість розпізнавання за рахунок зменшення кількості операції накладання літер одна на одну при порівнянні з еталоном.

Спочатку необхідно провести попереднє навчання для кожного окремого зразка почерку, створивши для цього необхідну базу з еталонами. Літери вписуються в прямокутник таким чином, щоб його сторони були дотичними до них. Літера, що показана на рис. 1.а – еталон, на рис. 1.б – літера, виділена з тексту за допомогою сегментації. Додатковою умовою на співставлення є однакові масштаби літер. Так як розмір виділеного сегменту для літери, яку необхідно розпізнати, та літери з бази можуть відрізнятися, то на другому кроці потрібно провести масштабування (рис. 1.в). Часто лінійні розміри виділеного сегменту та шаблону в горизонтальній та вертикальній площинах одночасно можуть не співпадати, так як навіть літери, написані однією людиною частково відрізняються. Однак достатньо співпадіння по горизонталі чи по вертикалі (рис. 1.а, 1.в).

Співставлення виділеного сегменту з еталонами відбувається таким чином, що їх центри мас співпадають (рис. 1.г). Літера, що має найбільше співпадіння із літерою з бази вважається її копією, а також може бути додана в базу для подальшого навчання.



а) б) в) г)

Рис. 1. Приклад зіставлених по горизонталі літер.

Запропонований метод надає можливість розпізнавати рукописний текст заданого зразку. Його перевагою є можливість порівняння літер, що не мають однакових лінійних розмірів. За рахунок того, що достатньо зіставити лише центри мас, підвищується швидкість точного накладання літер, за рахунок зменшення кількості накладань та взаємних зсувів зображень для правильного позиціонування.

Література

1. Кучуганов А. В., Лапинская Г. В. Распознавание рукописных текстов / А. В. Кучуганов, Г. В. Лапинская // Материалы международной научной конференции, Ижевск, 13–17 июля 2006. – С. 98 – 103.
2. Shafait F. Performance Comparison of Six Algorithms for Page Segmentation / F. Shafait, D. Keysers, T. Breuel // Image Understanding and Pattern Recognition (IUPR) research group. – 2006. – pp. 12.
3. Запрягаев С. А., Сорокин А. И. Сегментация рукописных и машинописных текстов методом диаграмм Воронного / С. А. Запрягаев, А. И. Сорокин // Вестник ВГУ, серия: системный анализ и информационные технологии, № 1, 2010. – С. 160 – 165.
4. Васильев С. Распознавание непрерывного рукописного текста в режиме off-line [Електронний ресурс]. – Режим доступу: https://geektimes.ru/post/136165/ – Електрон. тестові дані (дата доступу 02.03.2016).

УДК 004:931

РОЗПІЗНАВАННЯ ЕЛЕМЕНТІВ ОБЛИЧЧЯ ЛЮДИНИ НА ЗОБРАЖЕННІ

Шемшур Я. С., Штогріна О. С.
Інститут телекомунікаційних систем НТУУ «КПИ», Україна
E-mail: yarik33333@gmail.com, l_shtogrina@mail.ru

The recognition of the human face in the image

This paper provides a method of key face elements recognition. The main feature is to detect and recognize whole face first. This method includes methods of image recognition such as image binarization, contour facial recognition, image filtering. It improves speed of recognition because face elements must be found not in whole image, but only on detected face area.

Сьогодні розпізнавання людського обличчя використовується в багатьох сферах життєдіяльності, таких як медицина, охоронні системи, технології комп'ютерного зору та інтерфейси людина-комп'ютер для систем розумного будинку та мультимедійних пристроїв. Однак залишається ряд невирішених проблем, таких як складність обробки та низька точність, що спричинена різною мімікою людини, поганою освітленістю при зйомці зображення, різними кутами зору камери.

Існують такі методи розпізнавання обличчя: метод гнучкого порівняння на графах, використання нейронних мереж, метод головних компонент, активні моделі зовнішнього вигляду, метод порівняння еталонів, метод на основі оптичних потоків [1]. В більшості з них для розпізнавання обличчя необхідно знайти та виділити основні елементи обличчя, до яких відносяться очі, брови, ніс, губи та деколи вуха. Всі ці методи мають в своїй основі ресурсоємкі математичні алгоритми які забезпечують високу точність проте мають низьку швидкодію. Отже актуальною є задача розробки методу розпізнавання основних елементів людського обличчя, який дозволить скоротити час обробки зображення за рахунок попереднього виділення саме області обличчя та пошуку його складових тільки в цій зоні.

Для знаходження обличчя на зображенні можна використовувати метод, який дозволяє виділити частину зображення в якій присутній діапазон кольорів обмежений за деякими значеннями притаманними шкірі людини. Таким методом є бінаризація за порогом [2]. При бінаризації зображення інтенсивність кожного пікселя порівнюють з пороговим значенням, якщо інтенсивність пікселя більша, то такий піксель перетворюють на білий, в іншому випадку на чорний.

Для виділення обличчя як об’єкта використовують обробку границь зображення [3]. Є декілька основних алгоритмів виділення границь: оператор Кенні, Собеля, Лапласа, Робертса.

Щодо виділення основних елементів, використовують класичні методи фільтрації із радіолокації та обробки сигналів. Які дозволяють виділяти певні особливості зображення використовуючи менші обчислювальні потужності. Найпростішим з таких методів є згортка з довільною характеристичною функцією («Вейвлет-перетворення») [4]. До класичних перетворень відносяться вейвлет Хаара, Морле, мексиканська шляпа. Вейвлет-перетворення мають в своїй основі перетворення дискретного сигналу S таким чином, що на виході утворюються два сигнали. Один з них являє собою грубу версію вхідного сигналу, а інший містить інформацію для його відновлення. Ці сигнали розраховуються за наступними формулами:

$$a_i = \frac{S_{2i} + S_{2i+1}}{2},\ b_i = \frac{S_{2i} - S_{2i+1}}{2},$$

де a – груба версія вхідного сигналу, b – сигнал з інформацією для відновлення, S_{2i} та S_{2i+1} – елементи вхідного сигналу з відповідними індексами.

В роботі запропоновано метод розпізнавання основних елементів обличчя, особливістю якого є пошук їх не на всьому зображенні, а в попередньо визначеній області – області обличчя. Для пошуку саме елементів обличчя накладаються обмеження на якість зображення та розміщення обличчя. Обличчя має бути добре освітлене та повернуте в анфас до камери. Кут повороту обличчя в горизонтальній та вертикальній площині не повинен бути більше 45° та 30° відповідно.

Для визначення області обличчя та подальшого пошуку в ній елементів обличчя комбінуються методи розпізнавання зображень. На першому етапі виконується обробка зображення, яка націлена на виділення області шкіри людини методом бінаризації за порогом. Біла область відповідає шкірі людини.

Під час другого етапу, на зображені виділяються границі обличчя за допомогою оператору Кенні. Цей оператор обраний тому що він має високу швидкодію, а при застосуванні до зображення, попередньо обробленого за допомогою бінаризації забезпечує прийнятну якість. Обробка отриманих границь, для виділення обличчя як об’єкту, проводиться за допомогою ланцюгового коду Фрімена.

Третій етап – розпізнавання основних елементів на обличчі. Для цього обраний Вейвлет Хаара [5], тому що він дозволяє легко виділяти ключові особливості зміни яскравості пікселів. Наприклад, ніс на зображенні буде

світліший ніж область біля очей, рот або брови. Так само область між очами буде більш світла, ніж вся область ока вцілому. Під час обробки зображення, вхідний потік це матриця яскравості пікселів котрі розділяються на 2 групи: чорні та білі. Таким чином утворюються примітиви Хаара (рис. 1), за допомогою яких виділяються основні елементи обличчя, котрі явно вирізняються на зображенні.

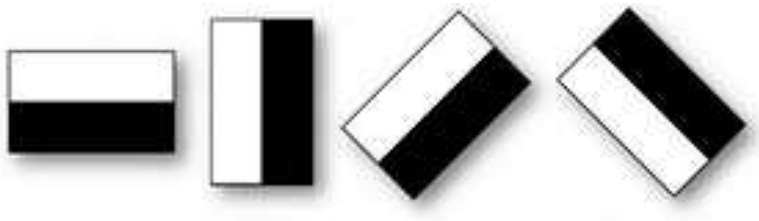


Рис. 1. Примітиви Хаара.

На основі запропонованого методу розпізнавання було розроблено програмне забезпечення для розпізнавання елементів людського обличчя, з використанням відкритої бібліотеки OpenCV та мови програмування C++. За допомогою утиліти CMake було виконано кроссплатформенну збірку розробленого програмного забезпечення для використання його на пристроях під керуванням операційних систем Unix чи Windows. За рахунок цього програму можна використовувати на слабких комп'ютерах, на основі однієї плати, таких як Raspberry Pi та ін. Використання компактних пристроїв дасть змогу створювати автоматичні системи розпізнавання. Наприклад, модулі для розпізнавання перехожих на дорозі, системи спостереження чи сигналізації та обчислення кількості людей в кімнаті чи будівлі.

Запропонований метод дозволяє підвищити швидкодію розпізнавання основних елементів людського обличчя на зображенні, за рахунок виділення меншої області для подальшої обробки зображення, та введення деяких обмежень на якість зображення. В подальшому планується застосувати метод розпізнавання елементів обличчя людини на відео.

Література

1. Горелик А. Л., Скрипкин В. А. Методы распознавания. - 4-е изд., 2004. - С. 200 - 262 с.
2. H.J.A.M. Heijmans, "Connected morphological operators for binary images", Computer Vision and Image Understanding, vol. 73, 1999. — pp. 99 - 120.
3. Duda R., Hart P. Pattern Classification and Scene Analysis. - John Wiley and Sons, 1973. pp. 270-272.
4. Lienhart, R. and Maydt, J., «An extended set of Haar-like features for rapid object detection», ICIP02, 2002. — pp. 900 - 903.
5. Messom, C.H. and Barczak, A.L.C., «Fast and Efficient Rotated Haar-like Features Using Rotated Integral Images», Australian Conference on Robotics and Automation (ACRA2006), 2006. pp. 1 - 6.

УДК 004.9

ИНТЕЛЛЕКТУАЛЬНАЯ ТЕХНОЛОГИЯ ОЦЕНКИ ПСИХОФИЗИЧЕСКОГО СОСТОЯНИЯ ЧЕЛОВЕКА

Косовненко Р. А., Штогрина О. С.
Институт телекоммуникационных систем НТУУ «КПИ», Украина
E-mail: kosovnenkoroman@hotmail.com, l_shtogrina@mail.ru

Smart technology assessment psychophysical state of person

This article describes the problem of long-term assessment of the human condition. As a solution of the problem offered software tool to automate the evaluation process of the human condition through the analysis of figures obtained during psychophysiological tests.

Сегодня в мире все больше внимания уделяется изучению психофизиологического состояния человека. Многолетние наблюдения за человеком психологами, позволили выделить множество параметров, от которых зависит общее состояние, возможность развития болезней, а также его поведение в коллективе [1]. Развитие технических средств дало возможность измерять и фиксировать множество не только психологических и физиологических параметров, а также параметров окружающей среды, и других имеющих влияние на организм человека. Данные параметры фиксируются с определенной периодичностью, а некоторые даже непрерывно. Это позволяет учитывать индивидуальные особенности человека, так как в данном случае важно именно отслеживание изменений. Обеспечивается возможность не только определять текущее состояние человека, но и делать прогнозы на будущее [2]. Однако, проблемой на сегодняшней день остается то, что анализ зафиксированных параметров и дальнейшую оценку состояния человека производят эксперты, которые основываются на собственном опыте. При принятии решения эксперт не может одновременно учитывать большое количество параметров, поэтому полученная оценка может содержать ошибки и быть субъективной. Теряется оперативность из-за необходимости задействования эксперта, а также возможности одновременно оценивать только одного исследуемого. Таким образом актуальной задачей является разработка интеллектуальной технологии, которая бы предоставляла возможность автоматизированной обработки информации о человеке и его окружении для оценки психофизиологического состояния человека.

Данная работа проводится в рамках исследования состояния зимовщиков на украинской антарктической станции «Академик Вернадский», проводимом Национальным антарктическим научным центром Министерства образования и науки Украины. Для решения поставленной задачи были выделены параметры, которые будут анализироваться. Данные параметры фиксируются для всех членов экспедиции до отправки, а также на протяжении всего времени пребывания в ней и предаются для анализа в НАНЦ Украины. Были получены необходимые знания от экспертов о том, как происходит оценка состояния человека, на основе которых были разработаны алгоритмы для автоматизации этого процесса. Разработаны программные средства, которые являются частью

интеллектуальной технологии оценки психофизиологического состояния человека.

Данные программные средства позволяют получать оценку состояния человека в автоматизированном режиме, а также предоставляют ряд дополнительных возможностей для экспертов при проведении дальнейшего углубленного анализа полученных результатов. Данные возможности предоставляются по средствам графического интерфейса, который позволяет наглядно отображать информацию за счет сведения ее в таблицы, для которых реализованы фильтры и сортировки, для повышения наглядности результатов строятся графики и диаграммы [3].

Одним из тестов для определения состояния человека является цветопреференциальный тест [4]. В данном тесте определяется цветопреференция человека в зависимости от порядка выбора предложенных цветов, на основе которой делается заключение о психофизиологическом состоянии. Как пример, на рис. 1 продемонстрирована часть пользовательского интерфейса, на которой отображены результаты прохождения данного теста группой людей. Каждая строка отвечает одному тесту. Эта информация сведена в таблицу, и для наглядности ее ячейки раскрашены определенными цветами, которые соответствуют порядку выбора цветов каждым из исследуемых. В последнем столбике отображена рассчитанная цветопреференция, которая является результатом для каждого теста. Эти результаты можно использовать для интерпретации состояния каждого из испытуемых. Для анализа общих тенденций проводятся сравнения результатов групп испытуемых. На рис. 2 в виде диаграммы продемонстрированы результаты сравнительного анализа цветовой преференции для двух групп исследуемых людей за несколько периодов времени. Данная диаграмма дает возможность наглядно проанализировать количество преференций в каждой категории и отследить динамику изменений.

Для разработки рассмотренных программных средств была выбрана платформа .NET, использовался язык программирования C#. Для хранения результатов используется MS SQL и JSON. Для возможности автономной работы был разработан программный модуль, который является WPF-приложением. Такое решение позволяет использовать разработанные программные средства без подключения к сети Интернет, а при наличии сети синхронизировать данные с порталом НАНЦ, на котором хранятся все данные исследований. Также были реализованы возможности экспорта данных в различные форматы, например, xls, которые могут понадобится для сопутствующих задач.

Человек	1	2	3	4	5	6	7	8	9	10	11	12	Результат теста
тест1	8	7	6	5	4	3	2	1	9	10	11	12	желтая
тест2	5	8	6	12	9	10	4	7	11	1	2	3	желтая
тест3	12	1	11	2	5	10	3	6	8	9	4	7	Смешанная
тест4	12	11	1	2	10	9	3	4	8	7	5	6	Красная
тест5	3	12	2	1	4	5	11	8	10	9	6	7	Смешанная
тест6	12	11	9	10	7	8	1	3	2	6	5	4	Красная

Рис.1 Пример части интерфейса пользователя: таблицы с результатами тестов

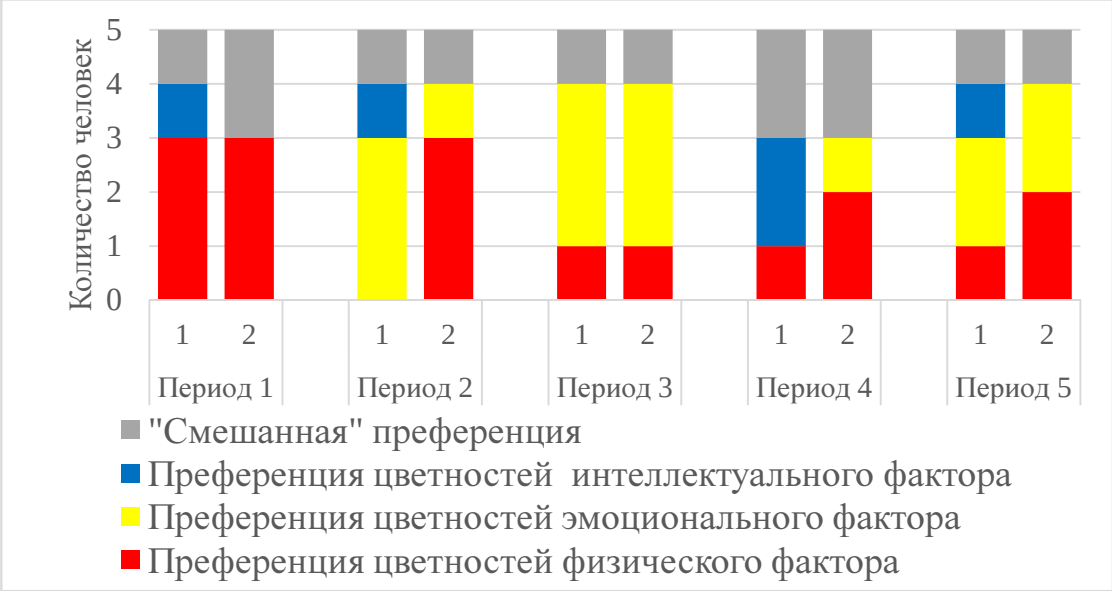


Рис.2 Диаграмма результатов сравнительного анализа цветовой преференции

Предложенная интеллектуальная технология позволяет автоматизировать процесс оценки состояния человека, за счет чего оперативно реагировать на изменения состояния и применять необходимые средства для его коррекции. Наличие наглядного графического интерфейса позволяет проводить дополнительные исследования экспертами для получения новых закономерностей. Дальнейшее развитие работы будет направлено на расширение функционала программных средств, за счет добавления возможностей сравнения результатов тестов и зафиксированных параметров с эталонными показателями, а также возможностей анализа с использованием статистических методов.

Литература

[1] Suciu G. Big Data Fusion for eHealth and Ambient Assisted. Living Cloud Applications / G. Suciu, R. Craciunescu, C. Butca, V. Suciu // 3rd International Black Sea Conference on Communications and Networking

[2] Kang K. Medical-Grade Quality of Service for Real-Time Mobile Healthcare / K. Kang, Wang Q., Hur J., Park K. – J., Sha L. // IEEE Computing in Healthcare Journal, February 2015

[3] Мадяр С.-А. И. Автоматизация анализа данных цветопреференциального обследования антарктических зимовщиков / С. - А. И. Мадяр, Е. Э. Ковалевская, Л. С. Глоба, Е. С. Штогрина, Р. А. Косовненко, Ю. А. Добров // Український Антарктичний Журнал, № 14, 2015. – С. 217 – 228

[4] Мадяр С. - А. И. Инновационные методы исследований в психофизиологии цветового восприятия: Методическое пособие / С. - А. И. Мадяр, Е. В. Моисеенко, Е. Э. Ковалевская // – К., 2015. – с. 1 – 30

УДК 004.72:621.39

ИСПОЛЬЗОВАНИЕ RASPBERRY PI ДЛЯ ВНЕДРЕНИЯ ДОПОЛНИТЕЛЬНОГО ФУНКЦИОНАЛА В СЕНСОРНОЙ СЕТИ

Воронюк М.М., Курдеча В.В., Плётка Б.С.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: bplotka.1996@gmail.com

USING A RASPBERRY PI TO IMPLEMENT ADDITIONAL FUNCTIONALITY IN THE SENSOR NETWORK

This article explane the use of high-performance microcontrollers as a basic element of wireless sensor networks for improved processing of information and increase of the network administrators effectiveness.

После более чем десяти лет интенсивных исследований и разработок, беспроводная технология сенсорных сетей появившись как возможное решение многих инновационных приложений. Беспроводной сенсорная сеть (БСС) имеет низкую стоимость, беспроводные сети из тысяч интеллектуальных узлов датчиков, которые кооперативно мониторинг физических или экологических условий, таких как температура, вибрация, давление, движение, влаги, света, или загрязнение окружающей среды в другом месте. Эти интеллектуальных датчиков образуют топологию сети через самоорганизации.

Датчики узлы могут передавать данные, обнаруженные их собственный датчик и может также передавать данные к соседним узлам. Одна из проблем возникающих в ходе разработки подобных сетей это эффективная обработка информации и дальнейшая её передача.

Для эффективной обработки полученной информации и последующей передачи полученной информации или статистики можно использовать высокопроизводительные микроконтоллеры, например Raspberry Pi. Подобное решение позволяет расширить функционал сенсорной сети, что можно показать на примере внедрения службы SMS-оповещения. В качестве средства для передачи информации предлагается использовать сеть Internet в стандартных ситуациях и службу SMS-оповещения в критических ситуациях или для передачи статистики.

Выбор Raspberry Pi как базового элемента сети обусловлен такими

факторами:

- Высокая производительность;
- Малые габариты;
- Низкая стоимость;
- Простота настройки и создания приложений;
- Возможность использования большого количества подключаемых модулей.

Схематически беспроводная сенсорная сеть с возможностью SMS-оповещения на основе Raspberry Pi требует интеграции многих аппаратных и программных компонентов. Система состоит из Raspberry Pi(базовой станции) и нескольких узлов состоящих из микроконтроллера, подключенных сенсоров и ZigBee передатчика(модуль Xbee). Узел в первую очередь ответственен за информацию собранную с датчика и управления им. Так же присутствует пользователь прикладной программы который осуществляет порядок передачи данных на базовою станцию.

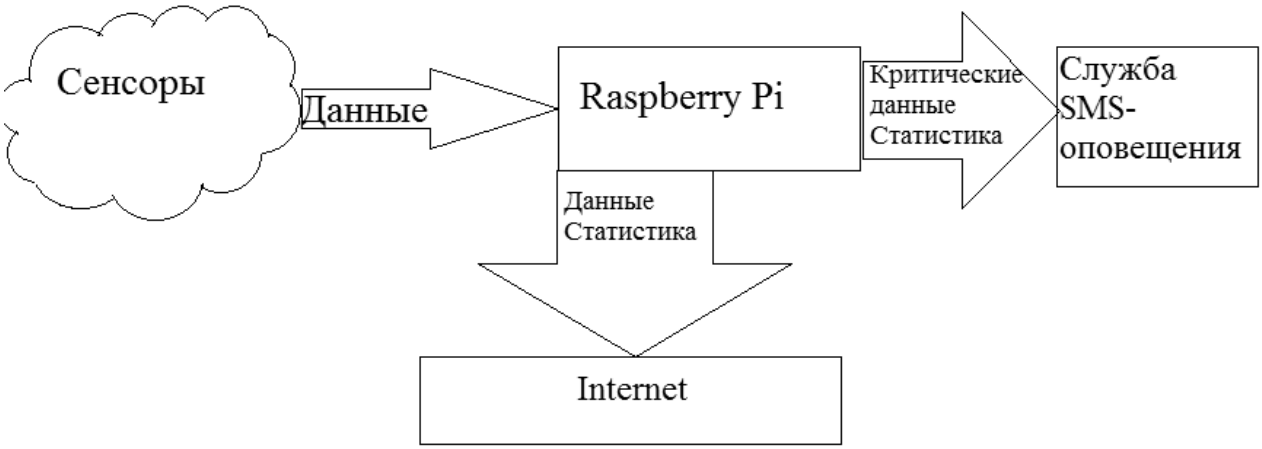


Рис.1 Внедрение дополнительного функционала
на примере системы SMS-оповещения.

На базовой станции осуществляется обработка полученой информации, формирование статистики, а так же обнаружение критических ситуаций. На основе результатов обработки принимается решение о среде передачи сообщений.

В этой системной архитектуре объединяется шлюз узел беспроводной сенсорной сети, сервер базы данных и веб сервер в одном одноплатный

компьютер (Raspberry Pi) аппаратных средств . Веб-приложение разработано для обеспечения пользователям удобный веб-интерфейс к системе.

Конечные пользователи или клиенты могут взаимодействовать с веб-приложением в пределах локальной сети или с любого терминала на Интернет для доступа к данным датчиков или выполнять дистанционное конфигурирование и управление развернутых узлов датчиков.

Система SMS-оповещения реализуется с использованием дополнительного GSM-модуля. Для того, чтобы получить сообщение SIM-карты помещается в GSMmodule и это связано с Raspberry Pi через последовательный порт RS-232 . Программное обеспечение предназначенное для чтение сообщений из модуля GSM и вставки их в базе данных на сайте. Raspberry Pi будет использовать эту функцию программы для чтения сообщений, используя только GSM модуль от разрешенных пользователей.

Таким образом, применение высокопроизводительных микроконтроллеров(Raspberry Pi) в качестве базовой станции БСС с возможностью SMS-оповещения имеет ряд преимуществ: низкая стоимость, низкое энергопотребление, компактность, масштабируемость, простота обслуживания.

Литература

1. Процедура оновлення програмного забезпечення в системі Software Defined Radio / Л. С. Глоба, В. В. Курдеча, С. В. Суліма // Вісник Харківського національного університету імені В. Н. Каразіна. Серія : Математичне моделювання. Інформаційні технології. Автоматизовані системи управління. - 2014. - № 1105, вип. 24. - С. 33-43. - Режим доступу: http://nbuv.gov.ua/UJRN/VKhIMAM_2014_1105_24_5
2. IEEE 802.15 WPAN Task Group 4 (TG4), available at http://www.ieee802.org/15/pub/TG4.html
3. Sarthak Jain, Anant Vaibhav and Lovely Goyal, "Raspberry Pi based Interactive Home Automation System through E-mail", International Conference on Reliability, Optimization and Information Technology-ICROlT 2014, India, Feb6-8 2014.

УДК 621.391+004.7

АЛГОРИТМ ВІДОБРАЖЕННЯ ТА ПЛАНУВАННЯ ВІРТУАЛІЗОВАНИХ ФУНКЦІЙ В МЕРЕЖІ МОБІЛЬНОГО ЗВ'ЯЗКУ

Суліма С. В., Скулиш М.А.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: lilthirteen@gmail.com

Algorithm for Mapping and Scheduling of Virtualised Functions in Mobile Network

The virtualization of mobile network is argued. The online virtual function mapping and scheduling problem is presented. The method can be used for the deployment management of virtual network functions on physical infrastructure to minimize operator costs and improving quality of service.

Сьогодні мобільні абоненти бажають залишатися на зв'язку в будь-якому місці, в будь-який час, і використовуючи будь-який пристрій. Принцип Network Functions Virtualization (NFV) спрямований на перетворення мережевих архітектур шляхом впровадження мережевих функцій в програмному забезпеченні, що може працювати на стандартній апаратній платформі. Предмет віртуалізованого EPC, що може динамічно реконфігуруватись, є досить новим сам по собі. Саме тому в цій сфері не так багато напрацювань.

Розподіл ресурсів в NFV мережах подібний до розміщення прикладних програм в датацентрах і хмарах [1]. Задача розміщення функцій також тісно пов'язана з вкладенням віртуальної мережі (Virtual Network Embedding – VNE) [2]. В останні роки багато наукових досліджень [3] розглядали проблему VNE або застосовуючи математичні моделі оптимізації або алгоритмічні підходи.

Ми розширюємо підхід VNE, визначаючи модель планування розташування мережевих функцій. Схожим чином [4] також фокусується на розгортанні віртуальних мережевих функцій, проте не враховує той факт, що ресурси можуть додаватися в процесі роботи. Крім того пропонується новий критерій оптимальності для жадібного алгоритму планування розташування віртуальних мережевих функцій. У цьому напрямку пропонується підхід до моделювання і дослідження динамічного виділення ресурсів для мережевих функцій у мережі телекомунікаційного оператора.

Задача виділення фізичних ресурсів в NFV може бути розділена на дві частини: (1) вкладення/відображення віртуальних машин на фізичні машини, яка пов'язана з VNE. Далі передбачається, що віртуальні вузли вже відображені на фізичні вузли. (2) відображення і планування віртуальної мережевої функції (Virtual Network Function – VNF) на створених віртуальних вузлах. Для задачі відображення і планування мережевих функцій (Network Function Mapping and Scheduling – NFMS) передбачається, що для даної віртуальної машини можливо обробляти декілька VNF, один за одним (можливо) з черги.

Тому NFMS складається з необхідності обробляти мережеві сервіси онлайн (кожен сервіс створюється і вбудовується в міру його необхідності) з використанням набору $F = \{1, ..., f\}$ з f віртуальних мережевих вузлів. Будь-який заданий сервіс мережі S складається з послідовності $SF = \{1, ..., m\}$ з m VNF, де функція $1 \le i \le m$ повинна бути оброблена на множині $F(i) \subseteq F$ вузлів. Функції $\{1,$

..., *m}* повинні бути оброблені одна за одною в певній послідовності, і кожен віртуальний вузол може обробляти не більше однієї функції одночасно. Час обробки для функції *i* на вузлі $j \in F(i)$ складає $\rho_{ij}>0$, де $1 \le j \le f$, і під час обробки або в черзі для обробки, функція *i* використовує буфер δ_i на вузлі, на який вона відображається. У будь-який момент, заданий вузол *j* має доступний розмір буфера B_j. Для кожної комбінації вузлів та функцій, визначаємо бінарну змінну $\beta_{i,j}$, яка приймає значення 1, якщо вузол *j* може обробляти функцію *i*, і 0 в іншому випадку. У цьому випадку задача полягає у виборі для кожної VNF *i* віртуального вузла $j \in F(i)$ і часу завершення t_i, коли її обробка буде завершена (час t_s, при якому обробка функції *i* на вузлі *j* починається, може бути отриманий з $t_s = t_i - \rho_{ij}$). Також визначаємо граничний термін t_l для обробки даного сервісу. Нарешті, для кожного віртуального вузла *j*, визначаємо очікуваний час завершення π_j останньої функції у черзі на обробку на вузлі, і для кожного сервісу визначаємо час прибуття t_a, який є часом, коли запит на відображення і планування сервісу отримується фізичною мережею.

Задачу NFMS можна розглядати як таку, що складається з двох частин: вирішення на які віртуальні вузли кожна VNF повинна бути відображена (проблема відображення), і для кожного вузла вирішення порядку, в якому відображені VNF повинні бути оброблені (проблема планування).

Алгоритм відображення та планування віртуальних мережевих функцій представлено на рис. 1 та рис. 2.

Алгоритм 1. Жадібне відображення функцій (S, F, C)
Старт
Здійснити резервне копіювання стану фізичної мережі
for $i \in S$ *do*
Ініціалізація: Множина можливих вузлів $F'=0$
if $(i=1)$ *then*
    $t_{i-1}=t_a$
end if
for $j \in F$ *do*
    $t_e=\rho_{ij}+max(\pi_j,t_{i-1})$
    if $((\beta_{ij}==1) \wedge (B_j \ge \delta_i) \wedge (t_e \le t_l))$ *then*
        $F'=F' \cup f$
    end if
end for
if $F' \equiv 0$ *then*
    Неуспіх відображення та планування
    Додавання VNF
    return
end if
    Відсортувати F' відповідно до C
    Обрати найвищий вузол j з F'*
    *Відобразити функцію i на j**
    Встановити $t_i=max(\pi_j,t_{i-1})$
    Оновити B_j, π_j, t_{i-1}
end for
Відображення та планування завершене
Кінець

Рис. 1 Алгоритм відображення мережевих функцій.

Алгоритм 2. Додавання VNF
$F=F\cup(f+1)$
$B_{f+1}=\delta_i$
$\pi_{f+1}=0$

Рис. 2 Алгоритм додавання мережевих функцій.

Алгоритм виконується наступним чином: після прибуття запиту на обслуговування, функції сервісу відображаються і диспетчеризуються послідовно. Для кожної функції *i* визначаються всі вузли $F(i) \subseteq F$, які мають можливість обробити її. Ці вузли потім ранжуються на основі жадібного критерію. Потім вузол з найкращим рангом обирається для відображення, а функція планується на обробку в кінці черги вузла. Фактичний час початку обробки основується і на доступності вузла (завершення обробки раніше поставлених в чергу функцій), і на завершенні обробки попередньої функції (якщо це застосовно). Крім того, на кожному етапі планування, визначається завершення обробки, щоб гарантувати, що воно знаходиться в межах встановленого граничного терміну для сервісу. Також цілком можливо, що під час відображення останньої функції сервісу час завершення перевищує граничний термін, або що функція не має жодного вузла-кандидата (через те, що всі вузли-кандидати повністю завантажені). У такому випадку пропонується здійснювати додавання ресурсів згідно з алгоритмом "Додавання VNF". На рис. 1 показується псевдокод алгоритму, де *C* позначає критерій, за яким ранжуються вузли.

Пропонується, що алгоритм базується на тому, що функції відображаються на вузли таким чином, щоб їх завантаженість була близькою до оптимального за критерієм енергоефективності значення.

У статті розглядається можливість віртуалізації мережі мобільного зв'язку. Представлено алгоритм управління виділенням ресурсів для задачі відображення та планування віртуалізованих мережевих функцій. Метод може застосовуватись при управлінні розгортанням віртуалізованих мережевих функцій на нижчерозташованій фізичній інфраструктурі для мінімізації витрат оператора зв'язку та покращення якості обслуговування абонентів.

Література

1. Jennings B. Resource management in clouds: Survey and research challenges / B Jennings, R Stadler // Journal of Network and Systems Management. – 2014. – pp. 1-53.
2. Fischer A. Virtual Network Embedding: A Survey / A. Fischer, J. Botero, M. Till Beck, H. de Meer and X. Hesselbach // IEEE Communications Surveys & Tutorials. – 2013. – Vol. 15, No. 4. – pp. 1888-1906.
3. Baumgartner A. Mobile core network virtualization: A model for combined virtual core network function placement and topology optimization / A. Baumgartner, V.S. Reddy, T. Bauschert // 2015 1st IEEE Conference on Network Softwarization (NetSoft). – London, 2015. – pp. 1-9.
4. Mijumbi R. Design and Evaluation of Algorithms for Mapping and Scheduling of Virtual Network Functions / R. Mijumbi, J. Serrat, J.-L. Gorricho, N. Bouten et al. // 2015 1st IEEE Conference on Network Softwarization (NetSoft). – London, 2015. – pp. 1-9.

УДК 621.3

ІНФОРМАЦІЙНО - КОМУНІКАЦІЙНЕ СЕРЕДОВИЩЕ СПІВРОБІТНИКІВ АНТАРКТИЧНОГО ЦЕНТРУ

Федяй Я.І., Новогрудська Р.Л.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: y.fedyai@mail.ru

Information - communication environment of employees of National Antarctic Scientific Center of Ukraine

This article describes the information - communication environment for employees of National Antarctic Scientific Center of Ukraine. The information - communication environment is presented in the form of a private office of the researcher on portal of National Antarctic Scientific Center of Ukraine.

Розробка та впровадження в Україні Національного Центру Антарктичних Даних шляхом побудови порталу знань антарктичних досліджень на основі сучасних технологій та середовищ створення порталів дозволяє розгорнути потужний портал знань, організовує його функціонування, а також визначає можливості забезпечення ефективного функціонування антарктичної станції "Академік Вернадський" при використанні супутникового зв'язку для надійної, безперервної передачі інформації з мінімальними витратами, встановлює інтерактивний зв'язок з антарктичною станцією "Академік Вернадський" та зацікавленими науковими установами в цілому [1]. Сьогодні Портал Національного Антарктичного Центру Даних (НАНД) використовується як єдина точка доступу, що реалізує задачі [2].

Створений портал НЦАД забезпечує вирішення наступних проблем:

- створення інформаційного банку даних для всіх досліджень, які виконуються НАНЦ;
- реалізація зберігання не лише даних але й знань, які здобуті в результаті досліджень на Антарктиді;
- надання доступу до інформації дослідникам, які перебувають в експедиціях;
- надання доступу до даних шляхом організації окремих категорій прав для різних груп співробітників;
- вдосконалення механізму систематизації та класифікації інформації;
- систематизація досліджень для організації ефективного пошуку даних різних категорій та предметних областей;
- організація якісного пошуку, не лише за ключовими словами, але й у знайомих користувачу термінах предметної області;

Діяльність працівників НАНЦ пов'язана з експедиціями, зустрічами, проведенням експериментів та участю у різноманітних конференції. Для підвищення ефективності взаємодії співробітників НАНЦ необхідно створити інформаційно-комунікаційне середовище на базі існуючого порталу в інтернеті. Портал НАНЦ розроблений на базі SharePoint2010, отже створення інформаційно – комунікаційного середовища дослідника не є складною задачею

адже технологією SharePoint передбачені стандартні засоби для реалізації колективної роботи та автоматизації робочих процесів порталу [3].

Інформаційно – комунікаційне середовище взаємодії співробітників НАНЦ буде представленим у вигляді персонального кабінету дослідника центру [4]. Провівши аналіз підходів до побудови кабінету дослідника та виділивши базові елементи та параметри взаємодії співробітників створено макет персонального кабінету, який відображений у вигляді блоків (рис. 1).

Рис.1 Макет персонального кабінету співробітника НАНЦ.

Інформаційний блок. Мета цього блоку полягає в висвітленні актуальної загальної інформації про дослідника, його освіту, науковий ступінь. Відображення інформації про специфіку його діяльності.

Блок «контакти» призначений для відображення контактних даних: телефон, e-mail, факс. Інформація цього блоку надає можливість встановлення зв’язку як між дослідниками центру так і партнерами.

Наукова діяльність. В НАНЦ існує багато напрямів досліджень і розробок. Основними напрямами досліджень є:

- геолого-геофізичні дослідження,
- океанографічні дослідження,
- гідрометеорологічні дослідження,
- геокосмічні дослідження,
- біологічні дослідження,
- медико-фізіологічні дослідження,

розроблення та впровадження нових технологій.

В даному блоці в залежності від напряму досліджень, якими займається власник електронного кабінету, буде відображена уся організаційна та наукова інформація та документація пов’язана з цим напрямком досліджень. Основне завдання Українських антарктичних експедицій - виконання заходів Державної цільової науково-технічної програми проведення досліджень в Антарктиці на 2011-2020 роки [5]. Кожен співробітник є учасником таких експедицій, тому в електронному кабінеті дослідника необхідно виділити розділ «експедиції», де будуть висвітленні матеріали про експедиції в яких він брав участь. Розділ міститиме організаційні документи, матеріали експедиції, фото, тощо. На порталі НАНЦ існує відповідний блок з інформацію про антарктичний журнал, а велика кількість робітників публікується в журналі, тому буде встановлений автоматизований зв’язок між блоком «публікації» в кабінеті дослідника і сторінкою антарктичного журналу на сайті. Тобто, при опублікуванні нової статті в журналі, вона буде відображатися в кабінеті відповідного дослідника. Цей зв'язок надасть можливість відображати публікацію в кабінеті дослідника при доданні публікації, що забезпечить ефективне зберігання ресурсів.

Проекти. В цьому розділі буде висвітлено міжнародні проекти, в яких приймають участь дослідники та науково - технічні проекти за державною цільовою-технічною програмою, а також відображено матеріали дослідника за цими проектами.

В блоці «Календар засідань» показано порядок денний, дату та місце проведення найближчого засідання, в якому приймає участь дослідник.

У роботі запропоновано базовий варіант структури кабінету дослідника НАНЦ, подальші дослідження будуть спрямовані на доопрацювання структури і її покращення, а також на безпосередню розробка цього кабінету на порталі НАНЦ, який буде працювати в тестовому режимі.

Література

1. Глоба Л.С., Мороз І. В., Новогрудская Р.Л., Мочалкина К.С., Кузін І.О.Создание единого информационного пространства данных антарктических исследований, Український Антарктичний Журнал, № 10-11, 2011, с. 343-351.
2. Глоба Л.С., В.М. Наконечний, Р.Л. Новогрудиська, О.О. Привар, Оптимізація функціонування порталу нанц при роботі з гетерогенними даними, VII Міжнародна Антарктична Конференція Антарктичні дослідження: нові горизонти та пріоритети”, Київ, 2015.
3. Microsoft about Share Point 2013 [Електронний ресурс] – Електр. Дані: http://technet.microsoft.com/en-us/library/ff607742%28v=office. 15%29 Дата доступу: 25.03.2016.
4. Microsoft about Share Point 2013 [Електронний ресурс] – Електр. Дані: http://technet.microsoft.com/en-us/library/ff607742%28v=office. 15%29 Дата доступу: 25.03.2016.
5. Кабінет Міністрів України; Розпорядження від 13.09.2001 № 422-р Про Державну програму проведення досліджень в Антарктиці на 2002-2010 роки 422-2001-р » Редакція від 13.09.2001, 1.45 Кб, 1 сторінка.

УДК 004.62

СИСТЕМЫ BIG DATA, ОСНОВНЫЕ ПОНЯТИЯ

Новогрудская Р.Л., Заика А.В.
Институт телекоммуникационных систем НТУУ «КПИ», Украина
E-mail: zaika.nastya7@gmail.com

Big Data systems, basic concepts

The basic characteristics of Big Data systems for storing and manipulating large amounts of data are described. The properties of the software platform for analytics large amounts of data as a set of tools of systems Big Data are specified.

На сегодняшний день широко распространенными являются системы Big Data. Понятие Big Data представляет собой серию подходов, инструментов и методов обработки структурированных и неструктурированных данных больших размеров для получения результатов, которые легко воспринимаются человеком. Эти системы стали очень популярными в последние годы из-за ряда преимуществ которыми они наделены. В работе описаны базовые понятия, связанные с построением систем Big Data.

К основным преимуществам использования систем Big Data можно отнести:

- Получение качественно новых знаний за счет комплексного анализа всей информации в едином аналитическом хранилище.
- Расширение функциональности существующих информационных систем поддержки бизнеса.
- Увеличение эффективности использования аппаратных ресурсов серверов.
- Обеспечение минимальной стоимости использования всех видов информации за счет возможности использования ПО с открытым кодом и облачных технологий хранения информации.

Системы BigData (SBD) это системы для хранения и манипулирования информацией, а также генерирования новых знаний на основании подхода BigData. Такие системы должны учитывать все особенности и характеристики BigData в рамках обеспечения доступа к информации сохраняя специфику информационных потоков в зависимости от предметной области и направления исследований пользователя.

Основной характеристикой SBD является территориальная распределенность больших объемов информации в разных областях жизнедеятельности человека.

Большие объемы данных определяется 5-ю основными характеристиками:

- объем – X1,
- скорость – X2,
- разнообразие – X3,
- стоимость – X4,

- сложность X5.

Учет таких характеристик при проектировании SBD предполагает минимизацию характеристик X4 и X5 с учетов постоянного возрастания X1, X2 и X3.

Основными особенностями больших объемов информации являются:

- территориальная распределенность информации,
- агрегация информации разных предметных областей и сфер жизнедеятельности пользователей.

Исходя из этого SBD должна включать:

- программные модули, построенные на основе интеллектуальных методов унификации информационных структурных единиц различных предметных областей,
- программные сервисы, реализующие интеграцию информационных и вычислительных ресурсов.

SBD должны предоставлять пользователю возможности работы с информацией, хранящейся в базах данных SBD, а также информацией, находящейся в открытом доступе глобальной сети (Рис. 1.1).

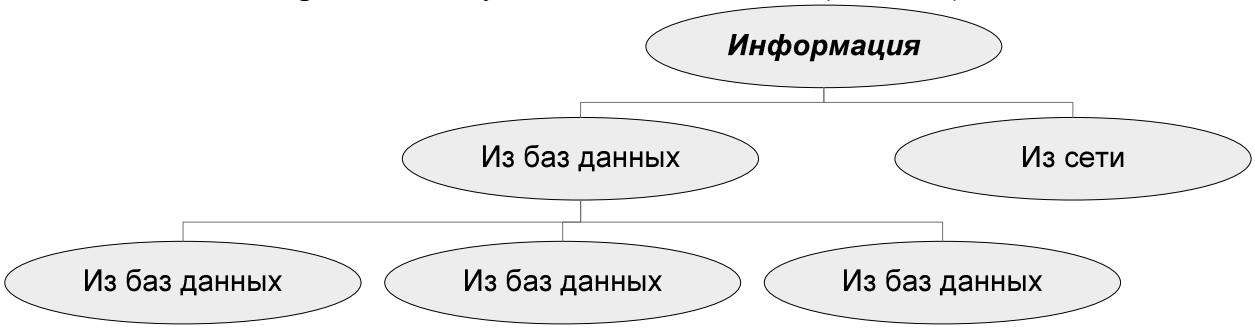


Рис. 1.1. Особенности хранения информации, представленной в SBD.

SBD предполагает манипулирование информацией в рамках выполнения следующих пользовательских функций: хранение информации, поиск, моделирование, аналитика и прогнозирование, а также выполнение расчетных заданий пользователей (Рис 1.2).

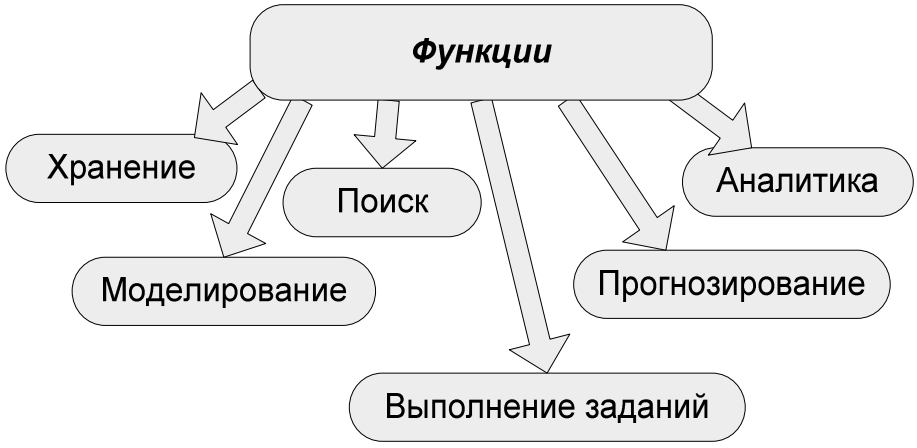


Рис. 1.2. Функциональные возможности SBD

Для осуществления таких функций в рамках комплекса инструментальных средств SBD необходимо разработать программную платформу аналитики больших объемов данных (BigData analytics platform) которая выполняет следующие функции:

- автоматический поиск и захват информации в Интернете в режиме реального времени, анализ информации (новости, BBS, блоги или другие средства массовой информации), например, поиск и анализ информации о наиболее горячих темах, которые обратили на себя внимание общественности, основываясь на ключевых словах поиска;
- прогнозирование тенденций развития новостных событий или прогнозирование возможности возникновения чрезвычайных ситуаций в социуме;
- интеллектуальный анализ имеющихся корпоративных информационных ресурсов, например, оперативный анализ, прогноз и технологическое предвиденье тенденций развития бизнеса в будущем, прогноз и технологическое предвиденье социально-экономического развития больших организационных систем.
- выполнение задач пользователей ориентированных определенную сферу деятельности учитывая специфические математические и расчетные методы предметной области.

Комплекс инструментальных средств SBD базируется на новых поколениях программных технологий и архитектур, а также средств программного обеспечения, предназначенных для извлечения экономической выгоды из очень больших объемов информации.

В работе описаны основные особенности, характеристики и функции систем Big Data, основываясь на которых становится возможным разработать специализированную программную платформу аналитики больших объемов данных выступающую как комплекс инструментальных средств SBD.

Литература

1. A. Halevy, P. Norvig, and F. Pereira, “The Unreasonable Effectiveness of Data,” IEEE Intelligent Systems, vol. 24, no. 2, 2009, pp. 8–12.
2. V. Gudivada, D. Rao, and V. Raghavan, “Renaissance in Data Management Systems: SQL, NoSQL, and NewSQL,” Computer (in press).
3. R. Baeza-Yates. “Big Data or Right Data?” Proc. 7th Alberto Mendelzon Int’l Workshop on Foundations of Data Management (AMW 13), 2013, vol. 1087, paper 14; *http://ceur-ws .org/Vol-1087/paper14.pdf*
4. C. Bizer et al., “The Meaningful Use of Big Data: Four Perspectives–Four Challenges,” SIGMOD Record, vol. 40, no. 4, 2012, pp. 56–60.
5. Дописувачі Вікіпедії. Big Data [Інтернет]. Вікіпедія, ; 2015 жов 7, [дата звернення 2016 бер 15]. Доступно з: *https://uk.wikipedia.org/w/index.php?title=Big_Data&oldid=16856338.*

УДК 621.39

СПОСІБ ОБРОБКИ ІНФОРМАЦІЇ В ВУЗЛАХ ІОТ ДЛЯ ЗМЕНШЕННЯ НАВАНТАЖЕННЯ НА СЕРВЕР ОБРОБКИ ІНФОРМАЦІЇ

Бугаєнко Ю.М.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: yura.buhaenko@gmail.com

Method for processing information in IoT to reduce server load

Creation architecture and approach of data processing in IoT node to reducing server and wireless network, based on programing solution, without updating hardware.

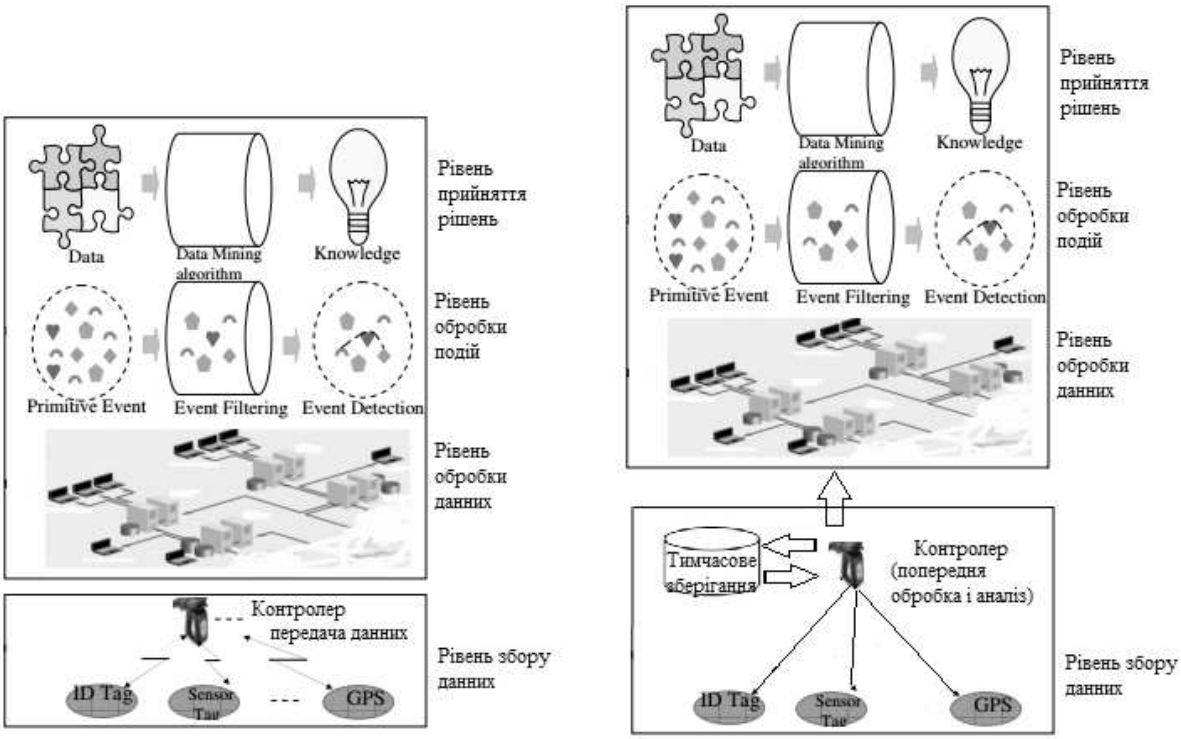
Інтернет речей (IoT) відноситься до наступного покоління Інтернету, що буде містити трильйони вузлів що є різними об'єктами, від малого датчика, смартфону і побутових приладів до великих веб-серверів і суперкомп'ютерних кластерів. Це поштовх до інтеграції і розвитку нових технологій обчислень і зв'язку (наприклад. сенсорних мереж, RFID-технології, технології мобільного зв'язку, розподілених обчислень, IPV6 і т.д.) і будує напрямок розвитку наступного покоління Інтернету. Але наразі цей новий напрям має ще дуже багато невирішених проблем, таких як: безпека, автономність, універсальність та проблема великих даних.

Сенсорні мережі і вузли IoT(Internet of Things) продукують величезні обсяги інформації, що генеруються з вбудованих або носимих розумних пристроїв. Отримати корисну інформацію з таких обсягів даних стає все важче, а проблема аналізу даних є однією із ключових на даному етапі розвитку інтернету речей. У деяких випадках, інтерактивне управління та обробка даних може знадобитися в реальному часі, наприклад в областях, що мають особливе значення, наприклад системи спостереження за здоров’ям чи системи безпеки. Але в інших випадках це не є визначальним фактором, тому використовуються різні методи для зменшення кількості оброблюваних даних задля зменшення навантаження на обчислювальну мережу. Головне завдання полягає в тому, щоб після аналізу і визначення сеансу, дані були представлені в стандартному вигляді та мали такий же результат після проходження систем прийняття рішень як і ті ж дані до обробки та оптимізації.

Є 2 великі групи методів для вирішення даної задачі: селекції та злиття. Перший є більш простим в реалізації але має великі неточності, а також може втрачати важливі дані. Цей метод частіше використовується для прогнозування, для того, щоб бути в змозі передбачити майбутні потреби споживачів і поведінку, засновані на даних, пов'язаних з поточними

тенденціями. Другий метод є більш точним, оскільки інформація не відкидається повністю, а лише «зливається» з записами, що лежать в допустимому діапазоні.

Ціллю даної роботи є створення нового способу на основі методу злиття даних, для зменшення навантаження на мережу, а також на серверну частину, де і обробляються великі обсяги даних. Головна ідея полягає в тому, щоб застосувати даний підхід ще на стороні вузлів IoT, а точніше на мікроконтроллері чи мікрокомп'ютері що зазвичай відповідає за передачу даних в систему обробки і прийняття рішень, тобто створити певний проміжний шар з обробки інформації перед її відправкою на сервер. Графічно даний підхід виглядає наступним чином (рис. 1):



а) б)

Рис. 1 Порівняння структури обробки даних в IoT
(а) існуючий варіант, (б) запропонований.

Сам спосіб обробки даних і прийняття рішення можна поділити на такі кроки:

- Вибір діапазону відхилення значень, відхилення за який вважатиметься важливим
- Отримання даних
- Порівняння отриманих записів з останніми збереженими
- Прийняття рішення про важливість даних

- Якщо дані були помічені як важливі, відправити на сервер
- Помістити запис на зберігання в пам'ять контролеру, зливши його з попередніми

При такій обробці ми матимемо зменшення на мережу, а також, що найголовніше, меншу кількість даних що надходити на сервер, при тій же якості останніх.

Перевагою даного методу є те, що реалізувати його можна без додавання нових додаткових фізичних пристроїв. Вся реалізація може бути втілена вже на існуючому контролері вузла. Для цього потрібно лише оновити програмне забезпечення останнього, а також врахувати меншу кількість вхідних даних на існуючих серверах.

Інтернет речей це концепція, яка в даний час тільки починає розвиватись, а ідея поєднати все і що завгодно і в будь-який час є привабливою, а динамічну природу IoT і масштаб, в якому вона буде функціонувати важко собі уявити, і тому, необхідно подолати всі наявні проблеми, однією з яких є проблема обробки великої кількості надлишкових даних, ще до глобального впровадження цієї концепції. При подальшому поширенні IoT, невпинно збільшуватиметься кількість приєднаних до нього вузлів та обсягів даних що вони продукують, тому вже зараз потрібно шукати підходи до оптимізації обробки інформації і вирішення даної проблеми, а одним із варіантів цілком може стати спосіб запропонований в даній статті.

Література

1. L. Mainetti, V. Mighali, and L. Patrono A Software Architecture Enabling the Web of Things // IEEE Internet of Things Journal - IEEE -Dec. 2015 -page(s) 445 – 454
2. M.A. Razzaque, Marija Milojevic-Jevric, Andrei Palade, Siobhan Clarke Middleware for Internet of Things: a Survey // IEEE Internet of Things Journal - IEEE - Feb. 2016 –page(s) 70 - 95
3. Shen Bin, Liu Yuan, Wang Xiaoyi Research on data mining models for the internet of things // Image Analysis and Signal Processing (IASP), 2010 International Conference - IEEE - April 2010 - page(s) 127 - 132

УДК 621.39

МУЛЬТИКРИТЕРИАЛЬНЫЙ МЕТОД ВЕРТИКАЛЬНОГО ХЕНДОВЕРА

Кирюшкин Р.А., Курдеча В.В.
Институт телекоммуникационных систем НТУУ «КПИ», Украина
E-mail: kirukysh@gmail.com

Multi-criteria Vertical Handover

In this paper analysis of a methods of vertical handover and is proposed implementation of Multi-Classifiers-Based Approach in the Heterogeneous Networks.

Вступление. Современные информационные технологии предоставляют широкий спектр высокоскоростных мультимедийных услуг и удовлетворяют потребности мобильных пользователей в этих услугах в любое время.

Вертикальный хендовер позволяет реализовать быстрое, плавное переключение между различными сетями, однако разработка и внедрение механизмов бесшовного хендовера является огромной проблемой и активной областью для исследований. Наиболее сложной задачей в вертикальном хендовере является минимизация потери данных и времени прерывания, в то время как мобильный терминал находится в прозрачном состоянии во время процессов переключения. Традиционные схемы принятия решений на основе одного критерия являются неэффективными из-за влияния неоднородности параметров сети и ее уникальных характеристик.

Алгоритмы и методы вертикального хендовера. Все алгоритмы могут быть распределены по нескольким категориям на основе используемых критериев принятия решений и методов обработки этих критериев:

1) Алгоритмы на основе RSS: Решение о выборе самой оптимальной сети принимается на основе мощности радиосигнала. RSS параметр сети-кандидата сравнивается с текущим параметром и выносится определенный вердикт. Является простейшим способом хендовера, но в то же время приводит к неэффективной передачи обслуживания, несбалансированной нагрузки и прерыванию.

2) Алгоритмы на основе пропускной способности: Решение принимается на основе того, удовлетворяют ли параметры пропускной способности новой сети нашим требованиям. Присутствует дополнительная задержка процесса сбора информации хендовера.

3) Алгоритмы, основанные на затратах: Для этих алгоритмов хендовера главным критерием является стоимость новой сети в совокупности с другими параметрами (например, стоимость, безопасность, доступная пропускная способность, потребляемая мощность, RSS). Имеют высокий уровень удовлетворенности пользователей, но в тоже время высокую сложность.

4) Комбинация алгоритмов: В этом типе используются объединение различных типов алгоритмов и нахождение компромиссного решения.

На сегодняшний день существует множество различных алгоритмов обработки классификаторов:

- Деревья решений;
- Метод на основе байесовых сетей;
- Искусственная нейронная сеть;
- Нечеткая логика;
- Объединение нескольких классификаторов.

Мультикритериальный метод вертикального хендовера. Различные атрибуты отличают неоднородные беспроводные сети друг от друга. Каждая беспроводная сеть может отличаться по покрытию, пропускной способности, мощности сигнала, скоростям передачи данных, задержке и т.д., следовательно, каждая из сетей поддерживает различные службы и устройства с требуемым из QoS.

Поскольку трудно найти логический компромисс между этими атрибутами, предлагается мультикритериальный метод вертикального хендовера на основе метода TOPSIS. Он предоставляет более чем одну целевую сеть в качестве альтернативных решений, а также обеспечивает гибкость в выборе критериев для решения о переходе в лучшую сеть. Комбинация классификаторов поможет в определении правильного решения о хендовере в неоднородных беспроводных сетях и поможет использовать преимущества различных беспроводных сетей [1-2].

Архитектура этого способа показана на рисунке 1:

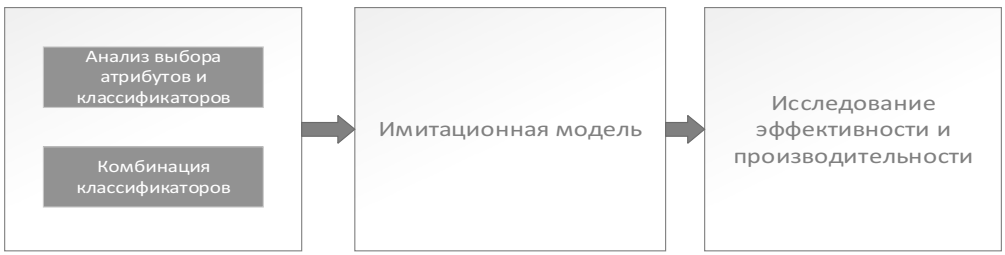


Рис. 1 Графическое представление архитектуры хендовера на основе мультикласификаторов.

Проведем более подробное описание архитектуры:

1) Анализ выбора атрибутов и классификаторов: Атрибуты являются инцидентами, дающими индикацию относительно необходимости применения хендовера. Для данной модели наиболее подходящими будут такие критерии: показатель уровня принимаемого сигнала (RSSI), класс трафика, скорость и размещение сети.

2) Комбинация классификаторов: Объединение многократных классификаторов значительно улучшит решение хендовера. Для достижения мульти-

критериальности будет использоваться метод сравнения критерия с идеальным решением (TOPSIS). Входные параметры алгоритма являются параметрами базовых станций (топологии сети и параметров радиосвязи) и параметры мобильных станций (класс скорости и типа трафика) [3].

3) Имитационная модель: Построение имитационной модели для оценки эффективности новых комбинированных классификаторов, изучение и исследование эффективности алгоритма. Также включает в себя рассмотрение нескольких иерархических беспроводных сетей и типов трафика с различными требованиями QoS, описание движения мобильных терминалов в конкретный момент времени определяя их положение, скорость и ускорение.

4) Исследование эффективности и производительности: Оценка результатов измерений сравнения предложенного подхода с классическими подходами на основе трех параметров эффективности: количество переключений хендовера во время активного вызова, показатель балансировки нагрузки и средняя вероятность блокировки.

По сравнению с другими методами, методика сравнения критерия с идеальным решением имеет ряд преимуществ. Она имеет концептуальную простоту и хорошую эффективность вычислений, а также имеет возможность измерять относительную производительность для каждой альтернативы. При моделировании, TOPSIS обеспечивает более высокую пропускную способность и уменьшает потерю пакетов.

Заключение. На сегодняшний день существует большое количество алгоритмов вертикального хендовера. Все они имеют свои достоинства и недостатки, и одним из самых сбалансированных является алгоритм на основе мультикритериального метода выбора классификаторов. Он обеспечивает максимально эффективное качество обслуживания современных абонентов мобильных сетей, иметь ряд преимуществ, таких как надежность (минимизация ошибочных решений), обеспечение гибкости, точности балансировки нагрузки для всех вовлеченных сетей, уменьшение вероятность блокирования сети.

Литература

1. Nasser M. Alotaibi, Sami S. Alwakeel, " A Multi-Classifiers-Based Approach for Vertical Handoff Process in Wireless Heterogeneous Networks: Retrospective and Prospective", Computer Engineering Department, College of Computer and Information Sciences.
2. Метод вибору мережі доступу в мобільній системі SDR при вертикальному хендовері / Л. С. Глоба, С. В. Суліма, В. В. Курдеча // Вісник Національного університету "Львівська політехніка". Радіоелектроніка та телекомунікації. - 2014. - № 796. - С. 69-74. - Режим доступу: http://nbuv.gov.ua/UJRN/VNULPPT_2014_796_13
3. Gita Mahardhika, Mahamod Ismail and Rosdiadee Nordin, "Vertical Handover Decision Algorithm using Multi-Criteria Metrics in Heterogeneous Wireless Network", Journal of Computer Networks and Communications, 2015, pp 1-9.

УДК 004.89

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ MAAS ДЛЯ ПОБУДОВИ «ХМАРНОГО» ДАТА-ЦЕНТРУ

Лящук А.А., Міночкін Д.А.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: aliashchuk@outlook.com

Using MaaS for "cloud" data-center deployment

Usage of Maas for problem solution of centralized management of data centers is discerned. Architecture of Maas and its benefits are presented.

На даний момент Україна знаходиться біля витоків нової епохи – епохи «хмарних» сервісів, інтерес до яких зростає з кожним роком. Зокрема один із найбільших операторів мобільного зв'язку в Україні "Vodafone", повідомляє про реалізацію інноваційного проекту по створення «віртуальних» робочих місць у власній роздрібній мережі [1].

За даними досліджень корпорації «СІБ» об'єм продажу «хмарних» сервісів українськими дата-центрами у 2014 році склав $4,6 млн або 55 млн грн. При цьому 75-80% з них припадає на модель IaaS (Infrastructure as a Service), 12–13% — на SaaS (Software as a Service), і 6–7% — на PaaS (Platform as a Service) [2]. За результатами іншого дослідження, що виконали оператор хмарних технологій De Novo та компанія IDC, використання хмарних сервісів веде до зменшення витрат на підтримку IT інфраструктури на 50% [3].

На даний час, актуальною тенденцією побудови дата-центрів є використання тисяч малопотужних серверів з низьким споживанням енергії, для підтримки яких виникає необхідність в простому способі установки програмного забезпечення.

Тому, темою роботи є дослідження ефективних засобів керування та моніторингу масштабних дата-центрів.

Одним із методів розгортання високо-масштабних дата-центрів є використання технології MaaS (Metal-as-a-Service), а саме її реалізації від компанії Canonical, підтримка якої включена до серверних ОС на базі Ubuntu Linux.

MaaS позиціонується як механізм для управління групами фізичних серверів, як єдиним хмарним ресурсом. Це дозволяє, в свою чергу, без особливих зусиль розгорнути поверх фізичної «хмари» такі хмарні сервіси як OpenStack або Hadoop. Областю застосування MaaS можуть стати сервери на

базі процесорів Atom, а в майбутньому також і економічні сервери на базі архітектури ARM, що відрізняються низьким енергоспоживанням.

MaaS надає мережеві механізми централізованого розгортання ОС, її автоматичного налаштування та встановлення заданого програмного забезпечення. Після цього, фізичні сервери перетворюються на «хмарні» вузли, які потім включаються в пул для динамічного розподілу [4].

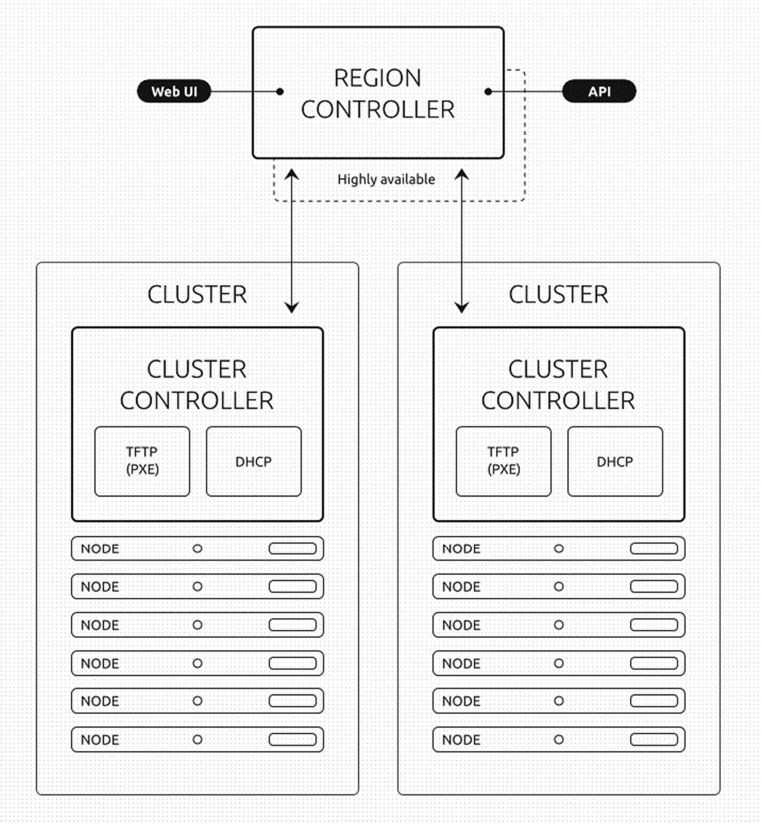


Рис. 1 Загальна структура роботи MAAS.

Архітектура MAAS спроектована з урахуванням можливості масштабування від декількох до тисяч серверів при необхідності. Ключові компоненти MAAS (Рис. 1):

- Region controller – головний сервер управління, що, окрім функцій управління інфраструктурою, надає API інтерфейс для доступу до хмари;

- Cluster controller(s) - сервер управління, що безпосередньо взаємодіє з вузлами хмари;

- Nodes – вузли, фізичні сервери.

Для невеликих інсталяцій (по кількості вузлів) можливе об’єднання функцій регіонального та кластерного управління на одному фізичному сервері. З іншого боку, при розподіленому розташуванні вузлів в декількох сегментах мережі, має сенс налаштування для кожного сегменту окремого Cluster controller.

За допомогою простого Web-інтерфейсу Region Controller дозволяє системним адміністраторам проводити налаштування та моніторинг роботи дата-центру. Крім того, MaaS Region Controller надає зручний REST API для доступу до основних функцій системи, а також для створення власного програмного забезпечення для управління або використання ресурсів дата-центру.

Після розгортання, MAAS може бути інтегрований з Canonical Juju, що являє собою інструментарій для управління розгортанням пакетів програмного забезпечення на вузлах пулу. З його допомогою можливе розгортання різноманітних клієнтських сервісів на фізичній хмарі шляхом використання стандартизованих сценаріїв.

Таким чином, на сьогоднішній день розвиток «хмарних» технологій є важливим для України, але існує проблема централізованого управління сучасними дата-центрами. Одним із методів вирішення даної проблеми є використання «хмарної» технології MaaS. Використання MaaS дозволяє спростити процедуру розгортання і моніторингу фізичних серверів у дата-центрі. Однак, існує ряд задач, зв’язаних з оптимізацією функціонування «хмарних» дата-центрів, які потребують подальшого дослідження. Тому, одним із напрямків подальшої роботи є створення приватного «хмарного» дата-центру з метою вирішення поставлених задач, а також дослідження можливості використання технології MaaS для побудови сучасних телекомунікаційних систем [5].

Література

1. МТС улучшает обслуживание абонентов с помощью технологии «облачных вычислений». [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: http://company.mts.ua/ru/news/press-relizy/4575-mts-uluchshaet-obsluzhivanie-abonentov-s-pomocshyu-tehnologii-oblachnyh-vychislenij/.
2. Кириллов И. «Облака» в Украине: как меняется рынок. «СЕТИ И БИЗНЕС» / Игорь Кириллов. // «СЕТИ И БИЗНЕС». – 2015. – С. 42–52.
3. Облачные сервисы в Украине: итоги исследования [Електронний ресурс] . – 2015. – Режим доступу до ресурсу: : http://hi-tech.ua/oblachnyie-servisyi-v-ukraine-itogi-issledovaniya/.
4. Shuttleworth M. Introducing Metal as a Service: provisioning for the hyperscale era [Електронний ресурс] / Mark Shuttleworth – Режим доступу до ресурсу: http://www.markshuttleworth.com/archives/1103.
5. Кравчук С. О. , Міночкін Д. А. Застосування розподілених обчислень в телекомунікаційних системах / С. О. Кравчук, Д. А. Міночкін. // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – 2015. – №50. – С. 41–44.

УДК 004.89

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ РАДІОІНТЕРФЕЙСУ НА БАЗІ MSC AXE-810

Кривошеїна А.В., Міночкін Д.А.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: nastyshin16@gmail.com

Improvement of efficiency of radio interface based on MSC AXE-810

Usage of interface for problem solution of sustainable usage of radio interface resourses. Activation algorithm of Gs-interface is represented.

На сьогоднішній день, неможливо уявити життя людства без доступу до мережі Інтернет. Доступ до мережі необхідний у будь-який час та у будь-якому місці. Тому, останні десятиліття швидкими темпами розвиваються технології мобільного зв’язку для збільшення швидкості передачі та якості обслуговування абонентів. Одним з напрямків використання повсюдного доступу до Інтернет є стрімко зростаючий ринок пристроїв «Інтернету речей» (Internet of Things) [1]. Однак, на території України є значний шар пристроїв IoT (банківські термінали, охоронні сигналізації та ін.) для яких не суттєве зростання швидкості передачі даних, що надають нові технології мобільного зв’язку. Для свого функціонування вони використовують технологію GSM та її пакетну надбудову GPRS [2] із-за більшої області покриття, дешевизни і доступності. Тому, важливо провести аналіз можливості підвищення ефективності та надійності послуги пакетної передачі даних GPRS за допомогою наявних інструментів мережі.

Ключовим компонентом стільникових мереж стандарту GSM, що забезпечує надання і координацію основних GSM-сервісів, є базова мережа GSM. Архітектура мережі GSM схожа з мережами фіксованого телефонного зв’язку, але існують додаткові функції, які необхідні для забезпечення мобільності абонентів, як в межах своєї мережі, так і в роумінгу. Для забезпечення сервісів пакетної передачі існує розширення базової мережі, відоме як базова мережа GPRS (GPRS Core Network). Це дозволяє мобільним пристроям отримувати доступ до таких сервісів, як доступ до мережі Інтернет [3].

Центральним вузлом базової мережі є центр мобільної комутації (Mobile Switching Center, MSC). MSC це спеціалізована автоматична телефонна станція, що забезпечує можливість зв'язку з комутацією каналів, управління мобільністю та надання сервісів GSM для мобільних пристроїв всередині зони свого обслуговування. MSC пов'язаний з усіма елементами мережі GSM, а також управляє ними. Для виконання поставленого завдання необхідно провести аналіз можливостей MSC для підвищення ефективності послуги пакетної передачі даних для пристроїв IoT.

Для аналізу була використана цифрова комутаційна система з програмним управлінням Ericsson AXE 810. AXE-810 являє собою сучасну

високопродуктивну цифрову телефонну комутаційну систему. Вона призначена для широкого спектру застосувань на телефонній мережі і може функціонувати як:

-місцева "міська" телефонна станція;

-транзитна телефонна станція;

-станція стільникового та рухомого зв'язку;

-вузли інтелектуальної та ділової мережі.

Розглянемо дану комутаційну систему як систему зв'язку, що діє в стандарті GSM, розрахована на її використання в різних сферах. Вона може надавати користувачам широкий діапазон послуг і можливість застосовувати різноманітне обладнання для передачі повідомлень і даних. Ефективна передача даних можлива за рахунок використання надбудови пакетної передачі даних GPRS.

Так як GPRS використовує загальний фізичний ресурс радіоінтерфейсу спільно з існуючими ресурсами системи GSM з комутацією каналів, то службу GPRS можна розглядати як накладену на мережу GSM. Це дозволяє використовувати одну і ту ж фізичну середу в стільниках як для передачі мови з комутацією каналів, так і для передачі даних з комутацією пакетів. Ресурси GPRS можуть виділятися під передачу даних динамічно в періоди, коли відсутня сесія передачі інформації з комутацією каналів. Для вирішення завдання збільшення ефективності використання ресурсів радіоінтерфесу необхідно проаналізувати архітектуру мережі GSM/GPRS.

Для підтримки функцій GPRS стандартизовано 9 нових інтерфейсів. Еталонна модель GPRS, зображена на малюнку 1, показує основні складові мереж GSM і GPRS, а також інтерфейси між ними.

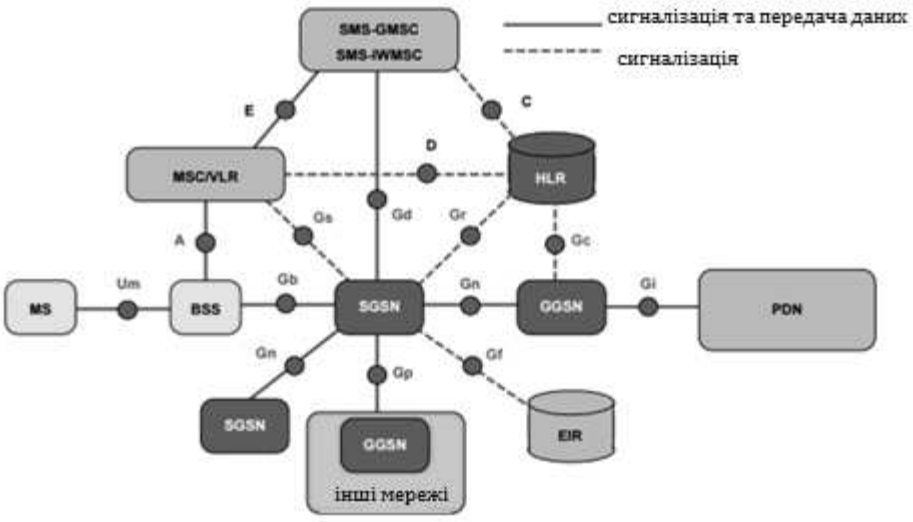


Рис 1 Еталонна модель мережі GSM/GPRS.

Інтерфейс Gi є точкою зв’язку між зовнішніми мережами PDN і мережею GSM / GPRS. Інтерфейс Gn служить для передачі отриманого із зовнішньої мережі пакета даних від GGSN до SGSN, в зоні обслуговування якого в даний час знаходиться абонент. Інтерфейс Gb служить для з'єднання

SGSN з BSS (PCU) і управління логічним зв'язком з мобільною станцією GPRS. Інтерфейси Gp і Gd є опціональними і використовуються між SGSN різних мереж і між SGSN і шлюзом SMS (SMS-GMSC / SMS-IWMSC), відповідно.

Крім того існує ряд суто сигнальних інтерфейсів. Інтерфейс Gr між вузлом SGSN і регістром HLR - обов'язковий інтерфейс. Інтерфейс Gc між вузлом GGSN і регістром HLR служить для запиту поточного місцезнаходження абонента при надходженні першого пакету даних в GGSN. При відсутності інтерфейсу Gc, запит може бути переданий через інтерфейс Gn на SGSN. який потім переправляє запит в HLR через інтерфейс Gr. Інтерфейс Gf між вузлом SGSN і регістром EIR - необов'язковий, оскільки регістр EIR є опціональним елементом в будь-яких мережах GSM. Інтерфейс Gs пов'язує MSC/VLR і SGSN і може використовуватися для загальних процедур, наприклад, поновлення розташування абонента. Якщо інтерфейс Gs не використовується, то процедури поновлення виконуються через радіоінтерфейс. Тому, використання інтерфейсу Gs дозволяє зменшити використання ресурсів радіоінтерфейсу.

Розглянемо Gs інтерфейс в якості можливості підвищення ефективності використання радіоінтерфейсу. Інтерфейс є опціональним в загальній архітектурі мережі GPRS / EDGE і фактично дозволяє проводити процедури регістрації та увімкнення функцій GPRS, тунелювання сигнальної інформації, виконання запитів щодо розташування абонента, тощо. Для аналізу була проведена процедура активації Gs інтерфейсу в SGSN в центрі комутації AXE-810. Після активації Gs інтерфейсу на ньому було увімкнено функції передачі інформації щодо місцезнаходження абонента та тунелювання сигналізації, не пов’язаної з GPRS. Це дозволило зменшити навантаження на радіоінтерфейс мережі.

Таким чином, активація Gs-інтерфейсу дозволяє зменшити витрати на сигналізацію в радіоінтерфейсі мережі GSM/GPRS. Однак, неправильний вибір параметрів Gs інтерфейсу може навпаки зменшити ефективність мережі в цілому, тому у наступній роботі буде проведено раціональний вибір параметрів Gs інтерфейсу для MSC AXE-810.

Література

1. Internet of Things (IoT) [Електронний ресурс].-Режим доступу до ресурсу: http://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html
2. Який принцип роботи GPRS [Електронний ресурс] . – 2015. – Режим доступу до ресурсу: http://www.radio-electronics.com/info/cellulartelecomms/gprs/gprs-network-architecture.php.
3. GPRS Network Architecture Tutorial[Електронний ресурс].-Режим доступу до ресурсу: http://www.radio-electronics.com/info/cellulartelecomms/gprs/gprs-network-architecture.php

УДК 004.75

ВИЗНАЧЕННЯ АНОМАЛЬНИХ СТАНІВ У РОБОТІ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ

Алєксєєв М.О., Безлюднов Д.Є.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: daniilbezludnov@gmail.com

Identifying anomaly states of the devices in IoT

Identifying anomaly states is complex problem that have a lot of different solutions. This paper describes how to detect anomalies in IoT sphere using Elman neural network.

На сьогоднішній день існує безліч розмов з приводу Інтернету речей (IoT). Інтернет речей - концепція комунікаційної мережі фізичних або віртуальних об'єктів, які мають технології для взаємодії між собою та з оточуючим середовищем, а також можуть виконувати певні дії без втручання людини. Дана концепція дозволяє змінити якість життя.

Кількість розумних пристроїв та протоколів їх взаємодії збільшується щодня, але всі ці пристрої працюють на різних платформах, мають різні служби та взаємодіють на основі різних протоколів та ін. Відсутні чітко прописані стандарти у цій сфері, що є причиною безлічі проблем (рис. 1), пов’язаних із сумісністю та нормальною взаємодією цих пристроїв. Існує безліч пристроїв, які через відсутність стандартів та наявності великої конкуренції у цій сфері взаємодіють лише з такими самими пристроями або пристроями, що виготовлені тим самим виробником.

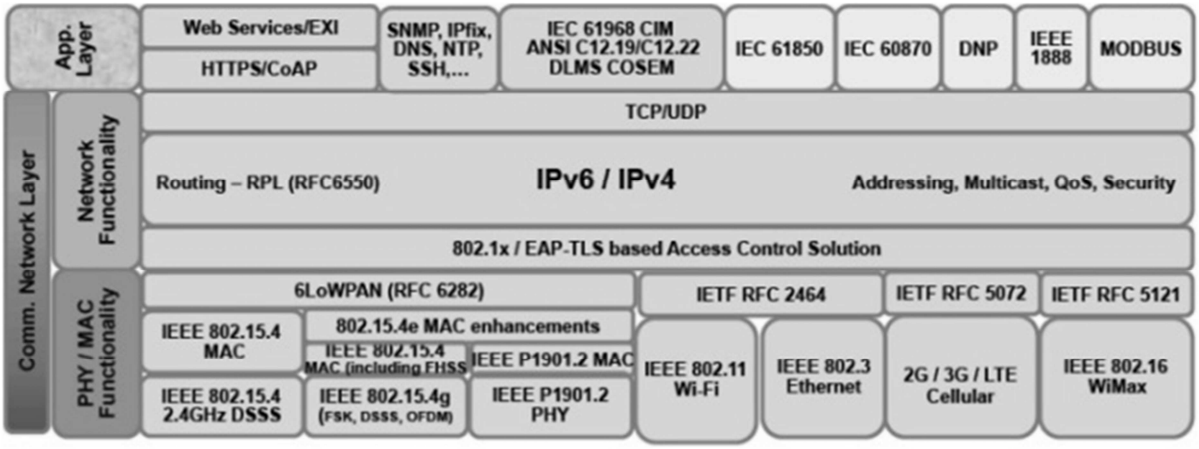


Рис. 1 Стек протоколів IoT.

Основною проблемою є велика кількість пристроїв, які працюють на абсолютно різних протоколах на всіх рівнях OSI (рис. 1). Різноманітність протоколів зв’язку, невеликі потужності у каналі зв’зку, вплив та нестабільність навколишнього середовища ускладнюють можливість детектування позаштатних ситуацій в режимах роботи пристроїв IoT. Також, негативно впливають на можливість детектування позаштатних ситуацій, великі об’єми даних та дуже часто високі швидкості надходження нових даних.

Якщо розглядати потік даних, то можна виділити наступні види аномалій (рис. 2):

- короткі аномалії;
- різкі зміни константних значень;
- сильні зміни у середньому значенні;
- великі зміни у амплітуді (зміни мінімуму та максимуму);
- непостійні зміни у “формі” або періодичності.

При визначенні аномалій треба виділяти певні “рівні”, чи є дана ситуація аномальна. Який рівень відхилення температури термодатчика від середнього значення можна назвати аномалією? 100%, 50%, 10% чи 1%? Через відсутність чітко визначених критеріїв введемо поняття шкали аномалій.

На шкалі аномалій можна виділити певні основні рівні відхилень:

1. Рівень шуму - рівень незначних відхилень від середніх значень;
2. Рівень змін - рівень на якому в потоці даних детектуються певні зміни, які ще не можна назвати аномальними (рівень перехідних процесів);
3. Рівень аномалій - рівень різких, непередбачуваних змін.

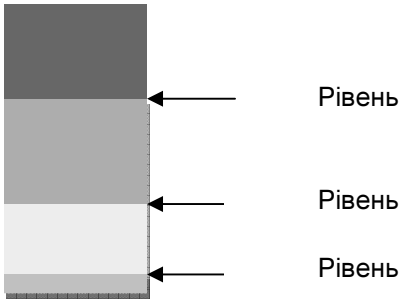


Рис. 2 Шкала аномалій.

Числові, або відсоткові (по відношенню до середнього значення) значення рівнів обираються під конкретні дані.

В середньому, значення по відношенню до середнього значення можна визначити наступними:

1. рівень шуму - 1..5-10%;
2. рівень змін - 11..30-50%;
3. рівень аномалій - >50%.

Детектування аномалій здійснюється за допомогою нейронної мережі Елмана (рис. 3) із блоком пам’яті, яка складається із наступних елементів:

1. Вхід - вхідний рівень перцептрону, кількість яких рівна розмірності вхідних даних (N);
2. Прихований рівень - проміжний рівень перцептрону, кількість нейронів на цьому рівні не менша за 2N (N входів та N обернених зв’язків);
3. Вихід - вихідний рівень нейронної мережі, кількість нейронів на цьому рівні може змінюватись від 1 до N;
4. Рівень керування, допоміжний прихований рівень нейронів, кількість нейронів рівна N;
5. Блок пам’яті - в найпростішому рішенні - черга довжиною T.

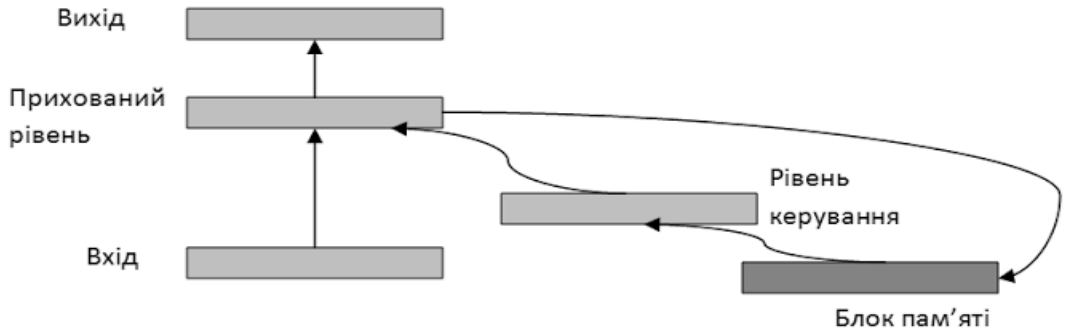


Рис. 3 Структурна схема нейронної мережі Елмана із блоком пам’яті.

Додавання блока пам’яті дає можливість детектувати зміни у порівнянні із попереднім значенням. Для цього раціонально використати від’ємні значення вагів на входах нейронах із рівня керування. Від’ємні значення, затримані на Т, підсумовуючись із виходами із вхідного слою дозволяють отримати дельту змін у потоці даних. В якості передаточних функцій використовуються сигмодальні функції, які дозволяють перейти від бінарних рішень до більш гнучких - відсоткових. Дані від передаточних функцій на вихідному рівні, які лежать у межах від 0 до 1 включно, накладені на певну шкалу можуть визначити із заданою достовірністю, наявність аномалій, змін у потоці даних або їх відсутність.

Запропонований метод детектування аномальних режимів роботи пристроїв IoT є застосовуваним до даної проблеми через:

1. Online`овість роботи, яка витікає у постійному відстежуванні надходжуванних даних, та зберіганні невеликої кількості «історії» даних;

2. Можливість роботи із будь-якими даними через те, що для порівняння використовується функція предикат, яку можна визначити маже на будь яких даних (числові, знакові, текстові, багатовимірні).

3. Простоту, так як метод базується на нейронній мережі Елмана, яка складається із порогових суматорів, зв’язків та блоку пам’яті, як зображено на *рис 3*, які уособлюють собою найпростіші математичні дії.

Проблема пошуку аномальних станів пристроїв досліджується вже давно. Однак розроблені методи погано застосовуються у сфері IoT через велику кількість даних різних типів. Розроблений метод детектування аномальних станів пристроїв IoT є ефективнішим у сфері IoT, ніж інші існуючи через його застосовуваність для будь-яких даних, online`овість та просту реалізацію.

Література

1. Y. Yaoa et al., Online Anomaly Detection for Sensor Systems: a Simple and Efficient Approach, Performance Evaluation, vol 00, pp. 1-24, 2010.
2. S. Rajasegarar et al.,"Distributed anomaly detection in wireless sensor networks in conf., ICCS, Florida, USA 2006.
3. B.Abhishek et al., Sensor Faults: Detection Methods and Prevalence in Real-World Datasetss, Trans.on Sensor Networks 6(3), 2010.
4. John A. (2015) Recurrent Neural Networks [Online]. Available: https://en.wikipedia.org/wiki/Recurrent_neural_network.

УДК 621.3

АУТЕНТИФИКАЦИЯ В РАСПРЕДЕЛЕННЫХ ГЕТЕРОГЕННЫХ СИСТЕМАХ С ДИНАМИЧЕСКОЙ АРХИТЕКТУРОЙ

Алексеев Н.А., Мазанка Р.М.
Институт телекоммуникационных систем НТУУ «КПИ», Украина
E-mail: alexeyev@its.kpi.ua, roman.mazanka@outlook.com

Authentication methods in distributed heterogeneous systems with dynamic architecture

With increasing amounts of data processing large amounts of information is becoming more difficult. The traditional way to solve this problem is to build dedicated high-performance distributed environments. Since the transmitted data must be protected against theft and distortion, the choice of authentication method that could effectively be used must be made. In this paper, the aim is to carry out an analytical review of the existing authentication methods.

С увеличением количества данных и ростом технического прогресса проблема обработки большого количества информации становится все более критичной. Традиционным, достаточно затратным способом решения данной проблемы является построение специализированных высокопроизводительных распределенных сред, таких как грид-системы или вычислительные кластеры. Одним из подходов к снижению материальных затрат при построении таких сред является использование неотчуждаемых некластеризованных распределенных вычислительных ресурсов, значительную долю которых составляют персональные устройства пользователей, подключенные посредством беспроводной сети. Поскольку передаваемые таким образом данные должны быть надежно защищены от кражи и искажения, выбор метода аутентификации, который мог бы эффективно использоваться при построении таких распределенных гетерогенных системах с динамической архитектурой является актуальной задачей. В данной работе ставится цель провести аналитический обзор существующих методов аутентификации с целью дальнейшего использования при построении систем такого рода, грид-систем персональных компьютеров (далее – ГСПК).

Рассмотрим самые распространенные методы аутентификации, которые поддерживаются большинством устройств, используемых в ГСПК: WEB-аутентификация, Media Access Control (MAC) filtering, Wired Equivalent Privacy (WEP), WPA2-PSK и 802.1x.

Wired Equivalent Privacy (WEP) – метод аутентификации, при котором один и тот же ключ (пароль) должен ввести каждый клиент сети. Поскольку сеть, использующая данный метод может быть легко скомпрометирована [http://arstechnica.com/gadgets/2007/04/new-attack-cracks-wep-in-record-time/], метод считается устаревшим и его использование не рекомендуется.

Еще один метод, который используется для защиты сетей – это Media Access Control (MAC) filtering – фильтрация по MAC адресу устройства. Достоинством этого метода является то, что точка доступа подключает лишь клиентов с известными ей MAC адресами. Данный метод аутентификации

может быть эффективен в малых сетях при использовании совместно с WEP. Но такой подход имеет существенный недостаток: MAC адрес может быть изменен пользователем, и тогда злоумышленник может перехватывать пакеты настоящего пользователя, или же совершать противоправные действия от его имени.

При использовании WEB-аутентификации во время подключения к беспроводной точке доступа у клиента запускается браузер и он попадает на страницу входа, где должен ввести свои учетные данные. При попытке перейти на другую страницу без прохождения процедуры аутентификации система автоматически перенаправляет пользователя на страницу входа. Такая система часто используется в публичных местах для уведомления пользователя об условиях предоставления услуг.

Wi-Fi Protected Access 2 Pre-Shared Key (WPA2-PSK) – это режим аутентификации, который предполагает ввод пароля каждым из клиентов, которые желают подключиться к сети. [http://www.juniper.net/techpubs/en_US/network-director1.1/topics/concept/wireless-wpa-psk-authentication.html] Данный метод является хорошим решением для домашней сети, но в корпоративной – его использование нежелательно, так как зная пароль, злоумышленник может перехватить передаваемый пакет и расшифровать данные. Другая сложность применения данного стандарта в корпоративной сети – невозможность централизованного администрирования беспроводного доступа: при необходимости администратор вынужден сменить пароль на каждой точке доступа, после чего каждый пользователь должен будет ввести его на своем устройстве. Необходимость смены пароля возникает довольно часто – при уходе сотрудника из компании, при краже или взломе устройства.

802.1x (также известна как Wi-Fi Protected Access 2 Enterprise (WPA2-Enterprise)) – протокол, который работает на основе портов. При подключении пользователя если авторизация прошла успешно, клиенту открывается виртуальный порт.

Таблица 1. Сравнение методов аутентификации.

Метод аутентификации	*WEP*	*Mac filtering*	*WEB-аутентификация*	*WPA2-PSK*	*802.1x*
Использование разных ключей для каждого пользователя / наличие фильтрации по адресу клиента	-	-	+	-	+
Простота администрирования	-	+	-	-	+
Отсутствие необходимости вмешательства пользователя при повторных подключениях	+	+	-	+	+
Обоснованность использования в корпоративном сегменте	-	-	-	-	+
Доступ к сети только для авторизированных пользователей	+	+	-	+	+
Сумма	2	3	1	2	5

Для анализа рассматриваемых методов приведем сравнительную таблицу 1. Проанализировав данную таблицу можем сделать вывод, что для корпоративной сети необходимо использовать технологию 802.1x. При подключении пользователя к беспроводной точке доступа, последняя отправляет EAP-Request – запрос на аутентификацию, клиентское устройство посылает EAP-Response – ответ, который перенаправляется на RADIUS сервер. RADIUS сервер отправляет пакет-запрос аутентификатору (коим является точка доступа), которая в свою очередь переупаковывает его в EAPOL и отправляет клиенту (в различных схемах количество таких сообщений может изменяться), клиент отвечает на запрос, ответ поступает на аутентификатор и перенаправляется на RADIUS сервер. В случае правильного ответа RADIUS сервер дает команду аутентификатору открыть порт.[http://citforum.ru/nets/articles/authentication/].

Таким образом, можно выделить следующие преимущества использования стандарта 802.1x:

- контроль на уровне сети (запрет доступа неавторизованным пользователям);
- может быть использован для проводных и беспроводных сетей;
- дает возможность разделять пользователей по VLAN-ам;
- динамическая смена ключей;
- невозможность перехвата трафика;
- IEEE 802.1x позволяет использовать несколько методов аутентификации – имя/пароль, сертификаты, tokens и т.д.

Во время тестового внедрении метода 802.1x в информационно-телекоммуникационную инфраструктуру Института телекоммуникационных систем НТУУ «КПИ» он подтвердил свою эффективность для использования в корпоративной среде и планируется для внедрения на постоянной основе.

Проанализировав различные методы аутентификации можно сделать вывод, что для построения гетерогенной системы с динамической архитектурой целесообразнее всего использовать стандарт 802.1x, так как он обеспечивает необходимую безопасность и дает возможность централизованно управлять подключением к распределенной системе.

Литература

1. Ars Technica. New attack cracks WEP in record – [Электронный ресурс] – Режим доступа: http://arstechnica.com/gadgets/2007/04/new-attack-cracks-wep-in-record-time– Электрон. текстовые данные (дата обращения: 26.03.2016).
2. Guniper Networks. Understanding WPA-PSK and WPA2-PSK Authentication – [Электронный ресурс] – Режим доступа: http://www.juniper.net/techpubs/en_US/network-director1.1/topics/concept/wireless-wpa-psk-authentication.html - Электрон. текстовые данные (дата обращения: 26.03.2016).
3. Сетевая аутентификация на практике – [Электронный ресурс] – Режим доступа: http://citforum.ru/nets/articles/authentication/ – Электрон. текстовые данные (дата обращения: 26.03.2016).

УДК 004.43

ОРГАНІЗАЦІЯ ВЗАЄМОДІЇ ПОРТАЛІВ НАНЦ ТА NASA НА БАЗІ REST-СЕРВІСУ

Глоба Л.С., Омельченко А.І.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: aomelchenko@its.kpi.ua

The approach to NANC and NASA portals interaction used REST-service

Methods and solutions for data exchange between the Ukrainian National Antarctic Data Centre and NASA portal are discussed. Two main options for the system architecture designing and their advantages and disadvantages are identified in the paper. The basic principles of data construction and their options, key architectural elements and basic functions are described. The approach for WEB-service designing is suggested based on the comparison two technologies (REST and SOAP).

На даний час проводиться значний обсяг наукових досліджень в Антарктиді в різноманітних галузях науки, вони є доступними лише вузькому колу вчених і фахівців. Дуже важливим негативним чинником процесу доступу до знань є погана систематизація і слабка структурованість великих обсягів інформації в існуючій на даний момент системі зберігання даних.

Створення Національного Центру Антарктичних Даних (НЦАД) Згідно з Резолюцією 4.1 XXII ATCM 1998 року вирішує задачі збору, збереження, обробки, передачі результатів антарктичних досліджень широкому колу науковців та науковим установам в Україні, а також зацікавленим закордонним науковим організаціям. Дані антарктичних досліджень представлено у відповідності до стандарту SCADM.

В рамках створення НЦАД пропонується підхід до передачі результатів антарктичних досліджень, отриманих українськими вченими на станції академік Вернадський, на портал NASA, що потребує створення відповідного web-сервісу. Результатом розробки моделі такого веб-сервісу та методу його функціонування стане автоматична передача інформації (яка включає дані, знання та результати антарктичних досліджень) на портал NASA, у відповідності зі структурою передбаченою всесвітньою організацією SCAR для відображення такої інформації [1].

Темою роботи є дослідження архітектурних рішень для побудови моделі веб-сервісу.

Для передачі даних в Global Change Master Directory (GCMD) використовується формат DIF(Directory Interchange Format). Цей формат є контейнером для елементів метаданих, з підтримкою валідації (перевірки

відповідності XML-схемі) обов'язкових полів, ключових слів, авторства тощо. Цей формат дозволяє користувачеві зрозуміти зміст набору даних і вміщує поля, які необхідні для прийняття рішення про те, який з наборів даних буде корисним для його наукових досліджень [2].

Можливі два основні варіанти архітектури системи надання доступу до даних: реалізація веб-сервісу, який передає повний обсяг даних від НАНЦ до порталу NASA або створення структури метаданих на порталі НАНЦ та веб-сервісу тільки для передачі метаданих до порталу NASA.

Другий варіант є більш бажаним, тому що дозволить зменшити обсяг трафіку, який передається мережею, але кількість звернень до даних у такому варіанті збільшується. Разом з тим, зменшується дублювання даних та вірогідність отримання некоректних даних через можливі завади в мережі, тому у стандарті SCADM рекомендовано передавати тільки метадані.

Процес передачі характеризується такими правилами. Клієнт на стороні порталу виконує тільки функції прийому введених даних форм, їх первинну перевірку та формування HTTP запиту. Простота цих функцій дозволяє реалізувати сервіс як на стороні сервера (server side), так і на клієнтській (client side, за допомогою мови JavaScript). Веб-сервіс, приймаючи запит від клієнта, виконує повну перевірку даних, перетворює їх в формат DIF і автоматично заповнює деякі з полів. Після цього він передає отриманий XML-документ в GCMD.

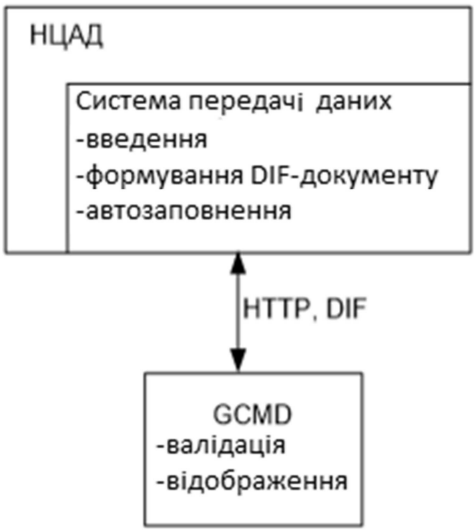


Рис 1. Архітектурна реалізація.

У варіанті, представленому на рис.1, всю роботу по перевірці даних, автоматичному заповненню полів, формуванню DIF-документа і передачі отриманого документа в GCMD виконує сам портал НЦАД. Такий підхід має більшу швидкодію і є більш безпечним порівняно з першим варіантом через відсутність обміну даними досліджень між веб-сервісом і порталами.

Однак вимоги міжнародного антарктичного співтовариства зобов'язують систему мати відкритий вихідний код, що є складним при використанні готового портального рішення (в даному випадку - SharePoint).

Для побудови веб-сервісу можливо використати також дві технології його побудови - REST і SOAP. Основна відмінність між двома підходами полягає в тому, що SOAP працює з операціями, а REST - з ресурсами та сценаріями їх використання[3]. Основними функціями веб-сервісу є перевірка даних і формування DIF-документа, що виконується значно швидше ніж SOAP через відсутність додаткових перетворень в формат XML. Крім того, для підвищення безпеки передачі даних в системі REST застосовує стандартні можливості протоколу HTTPS. Це підвищує безпеку передачі даних в системі. Оскільки система виконує функції конвертації і передачі даних (як ресурсів), застосовуючи певні алгоритми, то перевага надається технології REST.

Отже, в результаті проведених практичних досліджень запропоновано архітектуру системи надання даних для GCMD і визначено підхід щодо реалізації системи - на основі веб-сервісу для передачі метаданих антарктичних досліджень. Для реалізації такої системи було визначено переваги архітектури REST у порівнянні з технологією SOAP завдяки простоті використання, більшій швидкодії та можливості застосування стандартних протоколів без налаштувань.

Література

1. Oleksenko A.O., Globa L.S., Novogruds'ka R.L. Розробка процедури публікації метаданих в українському центрі антарктичних данних [Development of the metadata publication procedure in Ukrainian Antarctic Centre]. Naukovo-tehnichna konferencija "Problemy telekomunikacij": Materialy konferencii'. Kiev: NTUU "KPI", 2013, pp. 165 -167.
2. Directory Interchange Format (DIF) Writer's Guide. Availa-ble at: http://gcmd.gsfc.nasa.gov/add/difguide/index.html (accessed 28 April 2013).
3. Fielding R., Taylor R. Principled design of the modern Web architecture. ACM Transactions on Internet Technology. 2002, vol. 2. No 2, pp. 115 -150.

УДК 621.3

КЛАСИФІКАЦІЯ АЛГОРИТМІВ БАЛАНСУВАННЯ НАВАНТАЖЕННЯ ДЛЯ ВИКОРИСТАННЯ В РОЗПОДІЛЕНИХ ГЕТЕРОГЕННИХ МЕРЕЖАХ

Алєксєєв М.О., Гусак О.В.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: valavanca@gmail.com

Classification load balancing algorithms for use in distributed heterogeneous networks

This paper provides an overview of the classification load balancing algorithms for their further use and study. Also includes examples of algorithms and a brief review. Results generalized into the table.

При реалізації алгоритмів балансування потрібно знайти баланс між затримками при розподіленні завдань і обробкою самих завдань. Оптимальне рішення залежить від характеристики додатку, типу завдання, топології мережі і вузлів, вартості розгортання рішення. Для всіх цих проблем не існує ідеального алгоритму балансування який підходив би для будь-яких умовах, кожний підходить для конкретних складових і націлений на розв'язання чітких цілей. Необхідно провести класифікацію існуючих алгоритмів для того щоб використовувати наявні алгоритми максимально доцільно. Розробка такої класифікації стимулюватиме розробку нових алгоритмів і прискорить вдосконалення існуючих.

Для продуктивного і більш раціонального використання мереж з розподіленими розрахунками необхідно реалізувати дві вимоги які часто конкурують. Перш за все це те що процесори повинні бути зайняті корисною роботою. Другий пункт накладає вимоги до міжпроцесорного зв'язку – він повинен бути мінімальним. Для більшості розподілених систем розрахунку вартість налагодження контакту зростає при збільшені кількості і об'єму завдань. Важливо мінімізувати результуючу суму з них або максимум з них. Всі алгоритми балансування навантаження можна розділити на три групи: динамічні, статичні, адаптивні.

Динамічні алгоритми розподілення навантаження застосовують інформацію про стан системи для прийняття рішення про розподілення навантаження. Статичні алгоритми не слідкують за станом системи. В даній групі алгоритмів рішення про розподілення навантаження приймається заздалегідь і не змінюється в процесі роботи. Прикладом таких алгоритмів може слугувати RR (round robin), коли відбувається присвоєння задач до розрахункових вузлів по круговому циклу. Перша задача присвоюється першому розрахунковому вузлу друга другому і так до останнього вузла, потім все починається спочатку. Найбільш розповсюджена реалізація даного алгоритму на DNS-сервері шляхом повторення IP адрес вузлів в необхідній пропорції розподілення навантаження. Також до статичних відносять Simulated Annealing or Genetic Algorithms (генетичний алгоритм) який забезпечує змішану процедуру розподілу завдань за обчислювальними ресурсами з використанням методів оптимізації. Динамічне балансування передбачає перерозподіл розрахункової потужності на вузлах в ході

виконання програми і завдяки цьому можуть обігнати статичні алгоритми. Завдяки тому, що динамічні алгоритми відслідковують і аналізують такі параметри як завантаження розрахункових вузлів, пропускну здатність лінії, частоту обміну повідомленнями між логічними процесами, це призводить до збільшення накладних розрахунків на балансування в порівнянні із статичними алгоритмами.

Адаптивні ж алгоритми використовують поєднання двох вище наведених алгоритмів. В залежності від умов і поточних параметрів розрахункової системи вибирається найбільш доречний алгоритм. Наприклад Derbal[1] використовує масштабоване планування основане на ентропії розрахункової системи, а вже за допомогою ланцюгів Маркова сумує динамічні служби в мережі. Для прикладу є система[2] з підтримкою поколінь планування (the introduction of the Generational Scheduling) з реплікацією завдань. Цей алгоритм адаптується до змін в продуктивності з реструктуризацією завдань.

Відповідно до цілісності передачі завдання розділяють на витісняючи (preemptive) і невитісняючі (non-preemptive) алгоритми балансування. Не витісняючи алгоритми можуть передавати задачі які ще не почали розв’язувати. Витісняючи алгоритми здатні передавати задачі які розв’язані частково. Прикладом застосування не витісняючого алгоритму – сервер NetWare, витісняючого – ОС Windows NT, OS/2, VAX/VMS, UNIX.

Розділяють динамічні алгоритми балансування які враховують топологію і які її не враховують. По централізованості динамічні алгоритми розділяють на групи: централізовані, повністю розподілені, ієрархічні, суміщені.

Потенційно централізовані алгоритми менш надійні, ніж повністю розподілені, оскільки збій в роботі центрального компоненту призведе до збою всієї системи. Також центральний компонент потрібно забезпечити великою пропускною здатністю. Ієрархічні алгоритми частково вирішують ці проблеми, уникнути їх можна лише при повністю розподілених системах. Перевагою централізованого алгоритму є спрощення контролю і налагодження. Централізований спосіб підходить тільки тоді коли завдання може виконуватися незалежно і асинхронно відповідно до центрального процесора[3]. Необхідно мінімізувати обмін інформацією між центральним і підлеглим вузлом. Прикладом може слугувати алгоритм Least Load. Це динамічний алгоритм із зворотнім зв’язком. Завдання надсилається на той розрахунковий вузол який менш всього завантажений. Завантаженість може визначатися середнім часом відповіді.

У повністю розподіленій системі з N обчислювальними ресурсами для прийняття рішення про планування ресурс має обмінятись $2(N-1)$ повідомленнями[4]. Частковим прикладом для балансування такого типу може слугувати алгоритм[5] Ричарда Карпа (Richard Karp) який використовується для однорангових мереж (P2P). В даному алгоритмі інформація про однорангові вузли зберігається локально в каталогах кожного «едмеієнту» мережі. Таким чином значну частину проблем балансування було знято з сервера і передано на вузли.

Прикладом ієрархічної системи є мережа з проміжним забезпеченням gLite в якому система управління потоком знань(WMS) відповідає за

розподіл і управління завдань. WMS контролює процес виконання завдань і відправку результатів замовнику. В gLite для балансування навантаження використовується алгоритм «максимальної/нечіткої оцінки» які проводять відбір ресурсів по відповідності до поставлених задач. В суміщеній розподіленій системі на список завдань кожний розрахунковий вузол формує список доступних ресурсів. Актуальну інформацію про стан системи можна отримати як від кожного вузла напряму так і від центральної інформаційної системи. Така модель реалізована в проміжному забезпечені ARC проекту NorduGrid.

	ДИНАМІЧНИЙ				АДАП-ТИВНИЙ	СТАТИЧНИЙ
	Суміщений	Ієрархічний	Повністю розподілений	Централізований		
Genetic Algorithms						
RR						
Derbal						
The introduction of the Generational Scheduling						
Least Load						
алгоритм Richard Karp для P2P						
gLite (WMS)						
ARC (NorduGrid)						

Ця стаття поліпшує використання і вдосконалення алгоритмів балансування шляхом створення наглядної класифікації. Реалізовано короткий огляд найбільш розповсюджених алгоритмів з віднесенням їх до певної категорії. Кожний з підходів має свої переваги і недоліки і шляхом об'єднання і групування можна облегшити вибір необхідного алгоритму. Проявляється тенденція що чим складніша топологія і конфігурація мережі тим складніший алгоритм необхідно застосовувати.

Література

1. Derbal, Y.: Entropic Grid scheduling. J Grid Computing 4, 373–394 (2006)
2. Lucchese, F., Huerta, E.J., Yero, Sambatti, F.S.: Anadaptive scheduler for Grids. J Grid Computing 4, 1–17 (2006).
3. Bruce Hendrickson *, Karen Devine Dynamic load balancing in computational mechanics ст.488
4. Bokhari S. Partitioning Problems in Parallel, Pipelined, and Distributed Computing// IEEE Transactions Computers. — 1988. — 37, № 1. — P. 48–57.
5. Load Balancing in Dynamic Structured P2P Systems; Brighten Godfrey Karthik Lakshminarayanan Sonesh Surana Richard Karp Ion Stoica.

УДК 004.4

АЛГОРИТМ ДОДАТКОВОГО КРИПТОГРАФІЧНОГО ЗАХИСТУ ГОЛОСОВИХ ДАНИХ

Гончарова С. В., Могилевич Д. І.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: goncharovasabina@gmail.com

Additional cryptographic algorithm protection of voice data

This article describes the algorithm additional cryptographic protection of voice data in mobile network. The results of testing pseudo-random pattern generator are presented.

У наш час дуже велика кількість інформації передається через мобільні мережі, більшість з неї є голосовою. Об'єми інформації, що передаються, збільшуються весь час, деяка частина з цієї інформації є конфіденційною. Додатковий криптографічний захист голосових даних в мобільній мережі дозволить захистити інформацію, що передається, від зловмисника.

В роботі [1] розглянуто роботу різних програмних засобів додаткового криптографічного захисту голосових даних в мобільних мережах. Всі програмні засоби у своїй структурі за основу беруть протоколи VoIP, а саме, ZRTP та SRTP. Ці протоколи дозволяють проводити автентифікацію між абонентами та використовувати різні, підтримувані протоколами, криптографічні алгоритми в різних режимах для забезпечення захисту голосових даних. Протоколи ZRTP та SRTP, є вразливими, але деякі компанії, такі як Silent Circle, додають перевірки для усунення цих вразливостей, але це не повністю вирішує проблему і атаки стають лише менш ймовірними [2, 3].

Виходячи з вищесказаного, для захисту голосової інформації, було вирішено створити власне програмне забезпечення, як альтернативу існуючим. Без використання ZRTP протоколу, а використовуючи звичайні мережеві протоколи, з більш швидким алгоритмом шифрування голосових даних та нецентралізованою системою зберігання даних про користувачів.

Алгоритм працює в режимі клієнт – сервер, але кожен абонент виступає одночасно і клієнтом, і сервером. З'єднання створено за допомогою технології сокетів.

Програмне забезпечення є багатопоточним. Перший потік створюється при запуску програми, це сервер, який дозволяє іншим користувачам робити виклик на даний пристрій. Другий потік створюється під час виклику чи прийому виклику, це клієнт який з'єднується з сервером іншого абонента. Ще в двох потоках працює запис голосу у буфер та відтворення голосу, а також, окремим потоком працює процес шифрування. Шифрування здійснюється методом гамування.

Коли абонент з'єднується з іншим для розмови, то по каналу передаються секретні ключі для шифру гамування за допомогою асиметричної криптосистеми RSA.

Якщо процедура пройшла успішно, то починається розмова. Розмова йде за допомогою багатопоточного використання класів AudioTrack та MediaRecorder.

Використовуючи MediaRecorder, голосові дані з мікрофону записуються у буфер, де над цими даними проводиться шифрування методом гамування, після цієї операції дані передаються через мережу. Коли інший абонент отримує дані, він їх розшифровує та передає буфер до AudioTrack, який відтворює ці данні у звук з динаміка для розмов.

Схема роботи алгоритму показана на рис.1.

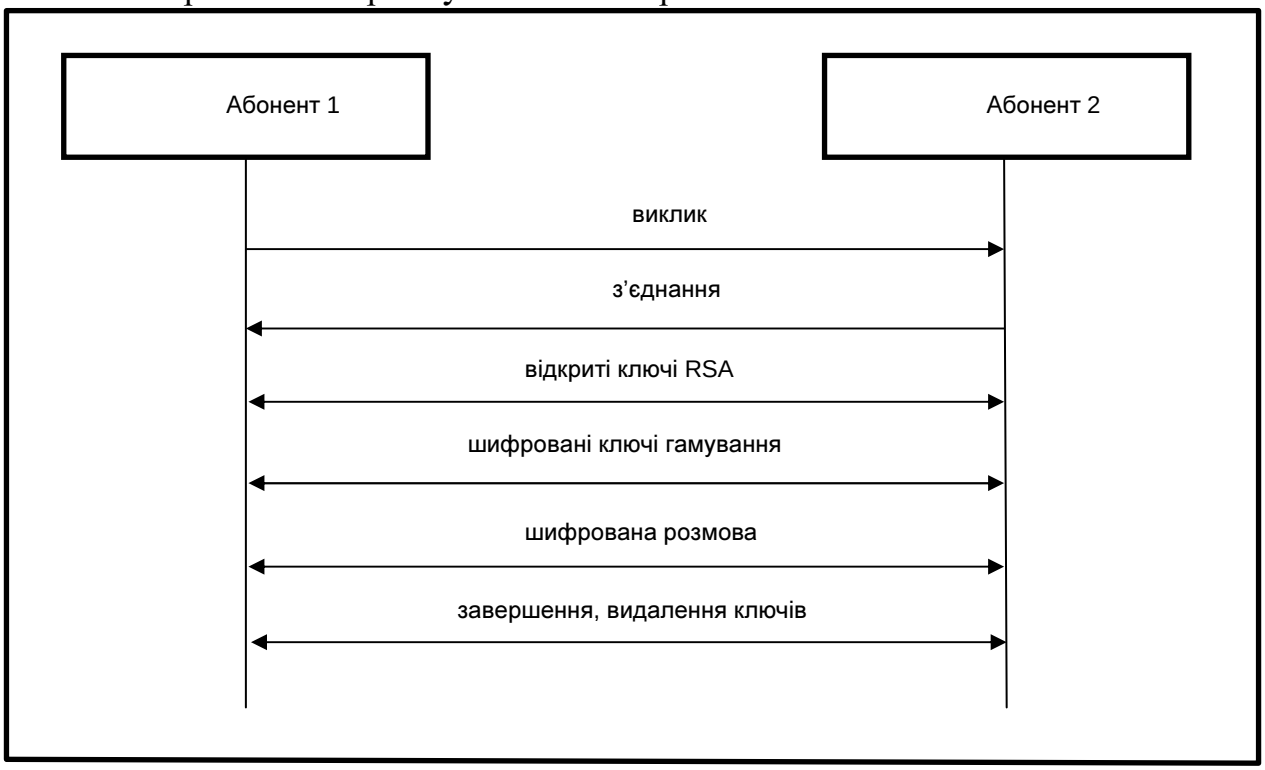


Рис. 1. Схема роботи алгоритму

Для генерації ключів було розроблено власний генератор псевдовипадкових послідовностей. Схема роботи генератора псевдовипадкових послідовностей показана на рис.2.

В якості джерела ентропії даного генератора псевдовипадкових послідовностей використовуються крайні праві дробової частини значень положень гіроскопу та акселерометру, зафіксовані в момент генерації. Гіроскоп та акселерометр фіксують положення в просторі та кут нахилу. Вони є достатньо випадковими так, як рухи кожної людини різні та гіроскопи і акселерометри в сучасних смартфонах настільки точні, що фіксують зміни, навіть, при вібрації руки людини. Кількість біт ентропії – 128, вони беруться по 32 крайніх біти з значення акселерометра та значень осей X, Y та Z гіроскопа.

Після отримання ентропії, ця послідовність подається на вхід булевій функції, яка має вигляд:

$$f(x_1, x_2, x_3, x_4) = x_2 \oplus x_4 \oplus x_2x_3 \oplus x_3x_4 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4$$

(1)

Це робиться для того, щоб зробити неможливим знаходження джерела ентропії сторонньою особою і, як наслідок, зробити можливим підробку ключів. Після використання булевої функції, вхідна послідовність скорочується до 32 біт. Щоб збільшити розмір входу використовується стандартний метод генерації псевдовипадкових чисел, а саме лінійно конгруентний.

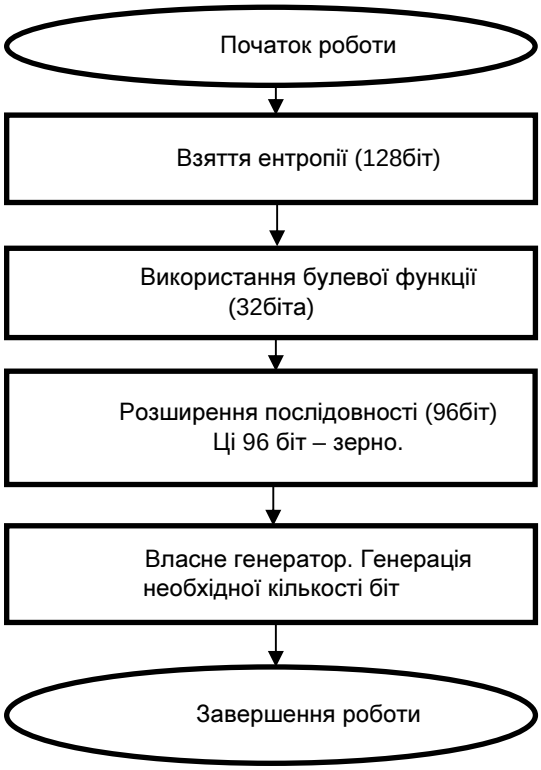


Рис. 2. Схема роботи генератора псевдовипадкових послідовностей

Генератор побудовано за схемою Геффе, але оскільки генератор Геффе не є стійким проти кореляційної атаки, використовуються не звичайні регістри зсуву з лінійним зворотнім зв’язком, а з доданою нелінійністю.

Над генератором псевдовипадкових послідовностей було проведено тестування. По-перше набір тестів DIEHARD на випадковість, по-друге тест на швидкодію генерації [4]. Генератор показав дуже добрі статистичні результати.

В роботі було проаналізовано недоліки різних програмних засобів додаткового криптографічного захисту голосових даних в мобільних мережах. Для усунення цих вразливостей було запропоновано алгоритм додаткового криптографічного захисту голосових даних. Для забезпечення роботи алгоритму було створено генератор псевдовипадкових послідовностей. Генератор протестовано на швидкодію та випадковість. Доведено, що генератор є захищеним від атак.

Література

1. Огляд на засоби криптографічного захисту [Електронний ресурс]. – Режим доступу : http://encrypted-phone-review.com/
2. Вразливості ZRTP [Електронний ресурс]. – Режим доступу : http://blog.azimuthsecurity.com/2013/06/attacking-crypto-phones-weaknesses-in.html
3. Офіційна сторінка SilentCircle [Електронний ресурс]. – Режим доступу : https://silentcircle.com
4. DIEHARD документація [Електронний ресурс]. – Режим доступу : http://stat.fsu.edu/pub/diehard/

УДК 621.395.74

ЗАХИСТ ГОЛОСОВИХ ДАНИХ В ПРОГРАМНО-АПАРАТНОМУ КОМПЛЕКСІ ASTERISK

Ткачук А. О., Могилевич Д. І.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: Dumenko.ann@gmail.com

Protection of voice data in hardware-software solution Asterisk

This article describes the main types of confidential information threats in Asterisk IP-telephony systems and proposes a set of measures to protect the voice data from malicious attacks.

Важливою подією в історії телекомунікацій стала поява технології передачі голосу по IP-мережі. Використання VoIP є сучасною тенденцією, це зручно, дешево, оскільки можна об'єднати віддалені офіси, не звертаючись до послуг операторів телефонного зв'язку [1]. Однією з таких VoIP технологій є програмно-апаратний комплекс Asterisk.

Asterisk є відкритою платформою марки Digium, що працює з різними операційними системами (Linux, Windows, FreeBSD, OS X) і дозволяє будувати і модифікувати телефонну станцію малих і середніх розмірів. Відкрита платформа означає ліцензійну програму з початковим текстом, не пов'язаним обмеженнями на подальшу модифікацію. Asterisk має усі функції класичної АТС, і навіть більше [2].

На сьогоднішній день, інформація є одним з найцінніших ресурсів, тому її захист – дуже важливе завдання. Чималу роль в роботі організації будь-якого рівня грають телефонні переговори. В силу зростаючої популярності IP-телефонії, все гостріше постає питання забезпечення її безпеки в загальному і конфіденційності розмов зокрема.

Знання основних джерел небезпеки для мереж IP-телефонії, а також розуміння методів усунення цих загроз допоможе зберегти репутацію і фінансові ресурси компаніям, що використовують Asterisk [3].

Перехват та маніпулювання даними є одним з найбільш вразливих місць телефонних мереж. У разі застосування IP-телефонії зловмиснику не обов'язково потрібен фізичний доступ до лінії передачі даних. Пристрій перехоплення, що знаходиться всередині корпоративної мережі з великою вірогідністю може бути виявлений, а зовнішнє прослуховування відстежити практично неможливо. Крім того, перехоплені дані або голос можуть бути передані далі зі змінами.

Відмова від використання або спрощення механізмів аутентифікації і авторизації в IP-телефонії відкриває для зловмисника можливість не санкціоновано отримати доступ до системи, підмінивши дані про користувача своїми. Можливий також злом облікових даних користувачів за допомогою перебору або прослуховування незахищених каналів зв'язку. Подібна вразливість може бути використана для здійснення дорогих дзвінків за рахунок

користувача, зводячи нанівець всю можливу вигоду від використання IP-телефонії. Також це може застосовуватися для запису перехоплених дзвінків на носії зловмисника з метою застосування даної інформації в корисливих цілях.

Ще одним з різновидів атак є «відмова в обслуговуванні» (Denial of Service, DoS). Ця атака націлена на перевищення граничного навантаження на систему великою кількістю коротких дзвінків або інформаційного «сміття». Без постійного відстеження ознак подібних атак і застосування пасивних засобів захисту, це призводить до того, що сервери IP-телефонії не справляються із збільшеним навантаженням і не можуть обслуговувати підключених абонентів.

При проектуванні будь-якої комунікаційної системи важливо розуміти, що жодне з самостійних технічних рішень безпеки не в змозі забезпечити абсолютний захист від усіх можливих загроз. Для цього необхідний комплексний підхід.

Ключовими критеріями захищеності інформації можна назвати конфіденційність, цілісність та доступність.

Найголовнішим для захисту інформації є налаштування самого серверу IP-телефонії. Для цього на сервері налаштовуються такі функції: використовується політика складних паролів; налаштовується відключення гостьових дзвінків; використовується система блокування доступу після невдалої спроби реєстрації; обмежуються направлення дзвінків, що доступні абонентам; виконуються регулярні перевірки системи на спробу злому [4].

В комплексі Asterisk також застосовуються міжмережеві екрани. Вони пропускають вихідний трафік від сервера телефонії до SIP-провайдеру і фільтрують вхідний трафік за певними правилами. Раціональним рішенням можна вважати закриття на міжмережевому екрані всіх мережевих портів для IP-телефонії, крім необхідних для її коректної роботи і адміністрування.

Для захисту конфіденційних переговорів і мінімізації можливості потрапляння конфіденційної і комерційної інформації в руки зловмисника, необхідно захистити передані по відкритих каналах зв'язку дані від перехоплення і прослуховування.

Оскільки для здійснення дзвінка клієнт і сервер попередньо обмінюються службовими даними для встановлення з'єднання, дану проблему можна розділити на дві складові - захист службових даних IP-телефонії та захист голосового трафіку. Найкраще використовувати протокол TLS (Transport Layer Security) для захисту SIP сигналів і протокол SRTP (Secure Real Time Protocol) для захисту голосового трафіку. Схема шифрування голосу в IP-телефонії показана на рисунку 1.

TLS - криптографічний протокол, що забезпечує захищену передачу даних між вузлами в мережі, є методом для шифрування SIP-протоколу. TLS забезпечує конфіденційність і цілісність інформації, що передається, здійснює аутентифікацію.

Після встановлення захищеного з'єднання починається передача голосових даних, убезпечити які дозволяє застосування протоколу SRTP. Протокол SRTP є одним з кращих способів захисту IP телефонії на базі IP-АТС Asterisk. Основна перевага цього протоколу - відсутність будь-якого впливу на якість зв'язку.

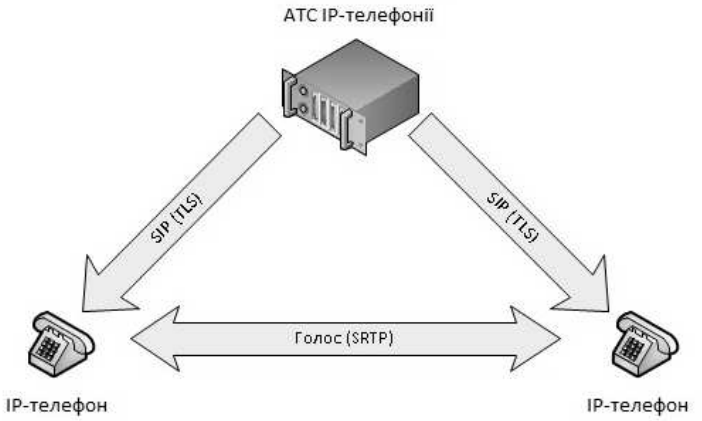


Рис. 1 Шифрування в IP-телефонії.

Але цього захисту може бути недостатньо для організації систем з підвищеними вимогами до захисту IP-телефонії (наприклад, для військових організацій). В таких випадках можна зашифрувати тунель, в якому буде передаватись голос, підключити віддалених користувачів через шифровані тунелі. Зміст перехоплених пакетів, відправлених по шифрованих тунелях буде відомий тільки власникам ключа шифрування. Цей же метод доцільно застосовувати для захисту підключень до постачальників послуг IP-телефонії. Це дозволить надійно передавати дані не лише всередині мережі, а також між віддаленими користувачами.

В роботі було проаналізовано атаки, які можуть загрожувати конфіденційності, цілісності та доступності інформації у VoIP системах. Для запобігання втраті інформації та захисту від можливих загроз, було запропоновано комплексний підхід. Він включає відповідні налаштування серверу VoIP, використання міжмережевих екранів, шифрування телефонних розмов. В результаті проведеного аналізу, пропонується використовувати поєднання протоколів TLS та SRTP для шифрування голосових даних в мережі. А також пропонується передавати голосові дані між віддаленими користувачами через зашифрований тунель. Використання всіх вищенаведених методів в комплексі забезпечить кращу безпеку інформації всередині мережі та з віддаленими користувачами.

Література

1. База знань Asterisk [Електронний ресурс]. – Режим доступу: http://asterisk.ru/knowledgebase.
2. Меггелен Дж., Мадсен Л., Сміт Дж. Asterisk: майбутнє телефонії, 2-е видання, Санкт – Петербург – Москва, 2009. — 652 с.
3. Безпека Asterisk [Електронний ресурс]. – Режим доступу : https://habrahabr.ru/post/188440/
4. Захист IP-телефонії [Електронний ресурс]. – Режим доступу: http://efsol.ru/articles/protection-ip-telephony.html.

УДК 621.3

СЕРВІС IFTTT ДЛЯ РОЗУМНОГО БУДИНКУ

Виговський М.С., Романов О.І.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: mvyhovsky@hotmail.com

Service IFTT for smart home

Prospective service IFTT to work with smart homes integrates all systems and provides incredible opportunities to control all home in general. This gives the smart home a greater degree of safety and comfort.

Останнім часом кількість «розумних» гаджетів, які підтримують сервіс IFTTT, стрімко збільшується. Але далеко не всі користувачі розуміють принцип функціонування цього сервісу. Коли справа доходить до автоматизації будинку, IFTTT може істотно полегшити життя власника - сервіс дозволяє об'єднувати окремі пристрої в єдину систему, причому робиться це швидко і достатньо просто.[1]

Принцип роботи IFTTT: сервіс пов'язує два сторонніх інтернет-додатки один з одним, в результаті чого певні події, що відбуваються з першим учасником тандему, викликають задану реакцію у другого учасника. Подібна логічна конструкція іменується «рецептом». Принцип роботи сервісу відображений в його назві: IFTTT розшифровується як «IF This Then That», тобто «якщо це, тоді те».[1].

Складові частини рецепта визначаються за допомогою так званих «каналів» - модулів, відповідальних за взаємодію з конкретним сервісом або «розумним» пристроєм. На даний момент таких налічується 160 штук. У кожного каналу є набір можливих подій, які поділяються на «тригери» і «дії». Тригер є свого роду спусковим гачком - умовою, при виконанні якої починає виконуватися задана дія. Найпростішим прикладом може служити підвищення температури за вікном до 30 градусів. Відповідно, дія - це та сама подія, яка слідує за спрацьовуванням тригера. Це може бути включення «розумної» розетки, до якої підключений кондиціонер. Будь-який рецепт складається з одного тригера і одного дії. Потрібно зауважити, що в базі даних IFTTT міститься безліч готових правил, так що створювати їх самостійно, найчастіше, немає потреби. І ця особливість стане в нагоді не тільки користувачам, які відчувають проблеми з логікою - серед представлених заготовок трапляються і дуже креативні рішення, які не кожному прийдуть на розум. [3].

Налаштування більшості рецептів здійснюється через сайт IFTTT, проте слід враховувати, що для роботи деяких каналів потрібно фірмовий мобільний додаток. При цьому ПЗ для iOS і Android дещо різниться по

функціоналу - в обох випадках є канали, недоступні конкуруючій платформі. В основному, бонусні можливості зав'язані на використанні GPS-передавача смартфона, а також вбудованих додатків (фотогалерея та список контактів).

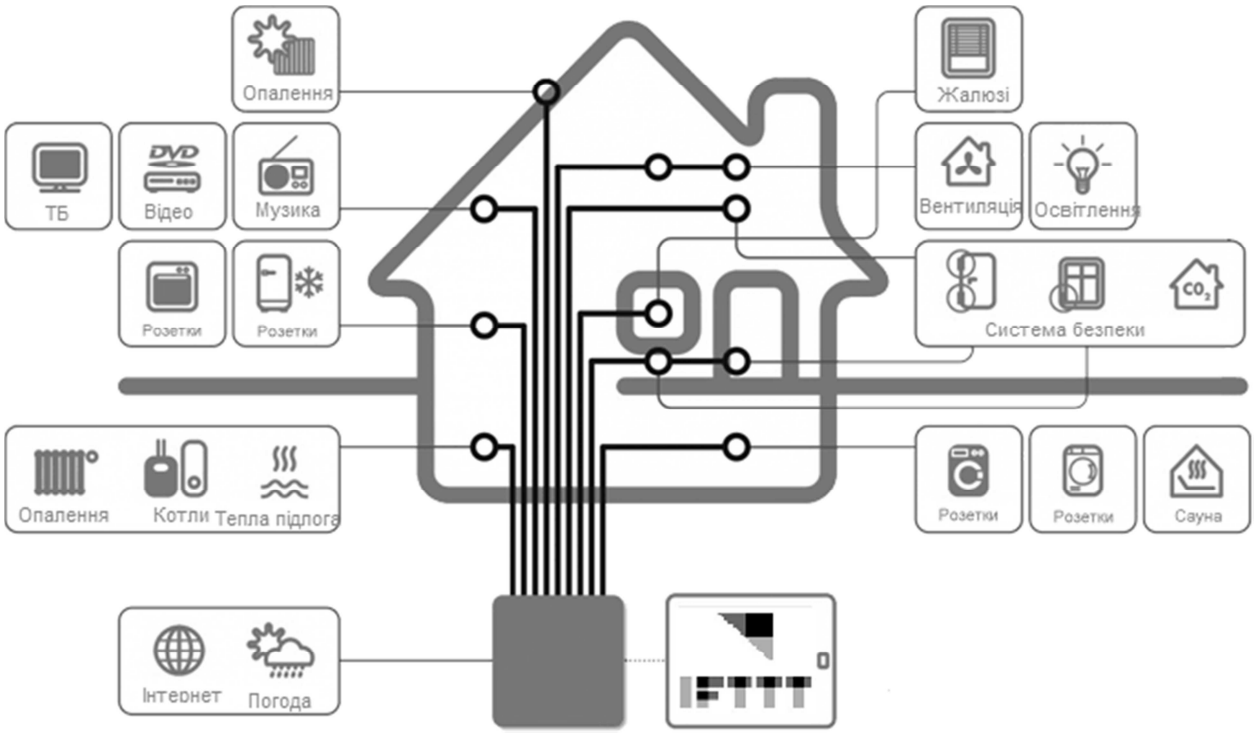


Рис. 1 Схема керування розумним будинком за допомогою IFTTT.

Головною задачею IFTTT являється забезпечення автоматизацією будинків всіх користувачів сервісу, та допомога у отриманні інформації про певний його стан, навіть якщо людина знаходиться на відстані від дому.

Сервіс IFTTT підтримує ряд готових систем автоматизації. В першу чергу це SmartThings. Для даної системи існує близько півтора десятка різних тригерів - практично будь-яка зміна ситуації в будинку може використовуватися для створення правил. Дії теж є - їх шість штук і пов'язані вони з включенням / відключенням системи, відкриттям / закриттям замків і активацією / деактивацією сирени. Revolv і Logitech Harmony Home також підтримують IFTTT, але можливості цих хабів куди скромніше - тригери для них відсутні. Також сервіс пропонує ряд каналів для пристроїв з сімейств Wink і Belkin WeMo. В останньому випадку список доступних інгредієнтів особливо добре опрацьований.[4].

IFTTT може використовуватися і для організації розумного освітлення. Наприклад, лампочки Philips Hue під впливом тригерів здатні включатися / вимикатися, мерехтіти, а також змінювати яскравість і колір. Світильник ORBneXt теж взаємодіє з IFTTT, але для нього список дій обмежений перемиканням кольору і видачею повідомлення на індикатор сповіщення. Найближчим часом до числа підтримуваних освітлювальних приладів повинні додатися і лампочки LIFX.[4].

Важливою частиною «розумного» будинку є продвинутий термостат. У даній категорії також є рішення з IFTTT. Зокрема, мова йде про іменитого Nest і двох пристроях від Honeywell, а саме Evohome і Single-zone. Для гаджетів Honeywell доступні лише дії. У їх конкурента, навпаки, акцент зроблений на тригерах, серед яких - вихід температури за встановлені рамки і перемикання режиму роботи. Мається на увазі, що термостат Nest може активно застосовуватися в рецептах, що враховують присутність / відсутність людей в будинку.[2].

При автоматизації будинку важливу роль відіграють сигнали оповіщення. Наприклад, IFTTT вміє здійснювати дзвінки і відправляти SMS на смартфон користувача при спрацьовуванні будь-якого тригера, причому ці функції не мають прив'язки до певної операційної системи. Інша функція відповідає за взаємодію з електронною поштою: сервіс дозволяє висилати повідомлення на email, а також активувати тригери шляхом відправки листів (будь-яких, або зі спеціальним заголовком) на сервер IFTTT. Gmail дозволяє запускати дії при одержанні листа, відповідно до заданих критеріїв. Не можна не згадати про функцію, що відповідає за погоду. Вона містить безліч різних тригерів, які враховують поточні кліматичні умови в конкретному місті, або прогноз на найближчу добу. У розрахунок може братися температура, вологість, швидкість вітру і загальний стан погоди. В окремих країнах доступні тригери, що враховують ультрафіолетовий індекс і зміст пилу в повітрі.

Технології все більше втручаються в наш світ. Сервіс IFTTT не є виключенням. Всі вище перераховані можливості роблять життя легшим, більш інформативним та безпечним. Вони допомагають економити електроенергію, контролювати власний будинок та знаходитися вдома з комфортом. Автоматизація будинку вже не є такою складною задачею для більшості людей.

Література

1. IFTTT [Електронний ресурс]. – 2012. – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/IFTTT.
2. Термостат Nest стал еще более умным [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: https://habrahabr.ru/company/medgadgets/blog/236323/.
3. Что такое IFTTT [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: http://blog.dusi.mobi/2015/12/22/ifttt/ .
4. Электроустановочные устройства умных домов [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: http://www.housecontrol.ru/material/29.php.

УДК 621.39

СИСТЕМА РОЗПОДІЛЕНИХ ОБЧИСЛЕНЬ GRID

Омельченко Р.Ю., Романов О.І.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: enternadore@ukr.net

System of distributed computing Grid

In this work the author has described a system of grid computing, also has indicated its tasks, structure and examples of application. Grid has been compared with similar systems and prospects of its application have been indicated.

У 1960 році піонер програмування Джон Маккарті пророчо говорив, що "обчислювальна діяльність може бути згодом організована як громадська послуга". У середині 1990-х років Ян Фостер і Карл Кессельман вели активну роботу в області об'єднання гетерогенних, географічно розподілених ресурсів в єдину інфраструктуру і запропонували термін, який став символом нової епохи комп'ютерних технологій – Grid. Grid - технологія створення географічно розподілених програмно-апаратних комп'ютерних інфраструктур, призначених для об'єднання обчислювальних потужностей з метою підвищення ефективності та надійності, зменшення витрат на придбання і підтримання, а також збільшення гнучкості використання різних ресурсів. [1]

Загалом, Grid - це об'єднання декількох комп'ютерів для вирішення єдиної обчислювально складної задачі, розбитої на підзадачі. Кожен комп'ютер вирішує кілька підзадач, а результати окремих обчислень об'єднуються. Основна перевага Grid в тому, що вона може складатися з комп'ютерів, що знаходяться один від одного на тисячі кілометрів і мають різні характеристики (як апаратні, так і програмні). Завдання об'єднання цих різнорідних комп'ютерів виконує проміжне програмне забезпечення, яке (віртуально) пов'язує всі комп'ютери через Інтернет в єдиний суперкомп'ютер. [2]

Дана технологія значно відрізняється від сучасних основних технологій розподілених обчислень, які не забезпечують вирішення виниклих проблем і не задовольняють вимоги координованого і динамічного розподілу ресурсів. Так, наприклад, технології корпоративних розподілених обчислень, такі, як CORBA (Common Object Request Broker Architecture) і EnterpriseJava, дозволяють розділяти ресурси, але тільки в межах однієї організації, можливості хмарних сервісів також не завжди дозволяють проводити обчислення, які потребують значних ресурсів. Радикально змінити картину можуть тільки Grid-технології [3]. Вони покликані вирішити наступні задачі:

- Масова обробка потоків даних великого обсягу;
- Моделювання складних процесів;
- Рішення дуже великих завдань, що вимагають величезних процесорних ресурсів, пам'яті і т.д.

- Колективні обчислення, в яких одночасно беруть участь користувачі з різних організацій [1].

Дані завдання можна вирішити за допомогою системи розподілених обчислень, загальна структура якої приведена нижче:

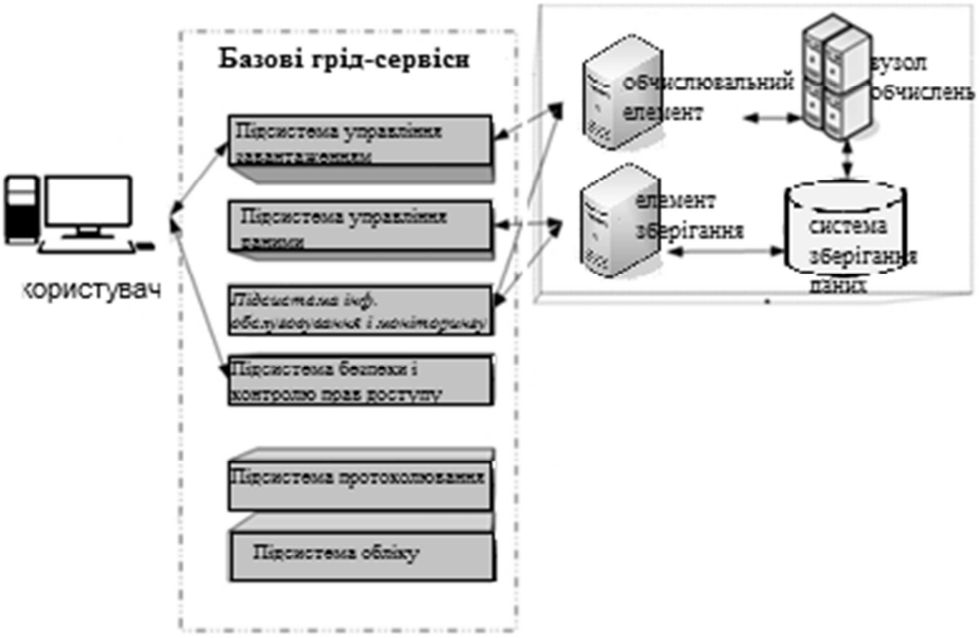


Рис.1 Структура Grid-системи.

Ресурсний центр включає в себе два типи ресурсів:

- Обчислювальні ресурси, на яких здійснюється виконання завдань;
- Ресурси зберігання даних, які забезпечують зберігання і транспортування даних між аналогічними ресурсами або даним ресурсом і користувачем в середовищі Grid.

Базові Grid-сервіси забезпечують роботу всієї Grid-системи і поділяються на наступні підсистеми:

Підсистема управління завантаженням. Вона управляє завданнями, запущеними користувачами, здійснює пошук ресурсів, запитаних завданням, і планує виконання завдання на відповідному обчислювальному кластері. Також вона стежить за статусом виконання завдання і дозволяє користувачеві отримати результат після його виконання.

Підсистема управління даними. Забезпечує доступ до систем зберігання різних видів, існуючих в ресурсних центрах. Складається зі служби файлового каталогу і служби каталогу метаданих.

Підсистема інформаційного обслуговування та моніторингу. Вирішує задачу збору і управління даними про стан Grid-інфраструктури.

Підсистема безпеки і контролю прав доступу.У завдання цієї підсистеми входить забезпечення аутентифікації і авторизації між різними компонентами Grid-системи.

Підсистема протоколювання відстежує процес виконання завдань.

Підсистема обліку призначена для обліку використання обчислювальних ресурсів.[4]

В даний час дослідники з цілого ряду наукових і виробничих областей використовують Grid-інфраструктуру для вирішення своїх задач. Серед прикладів реалізації слід виділити наступні:

1. Проект LCG (Large Hadron Collider Computing Grid) - використання Grid-середовища для моделювання та обробки даних із експериментів з елементарними частинками у Великому адронному коллайдері (до 15 ПБ/рік). Потік даних з детекторів коллайдера складає близько 300 ГБ/с, потім системою Grid фільтруються дані, що містять науковий інтерес, після чого вони зі швидкістю близько 300 МБ/с передаються на вузли обчислень;
2. Застосування в області астрофізики, які пов'язані з обробкою даних з телескопа MAGIC і з супутника Planck, запущеного Європейським космічним агенством;
3. Проект DrugDiscovery, Grid-інфраструктура якого обробляє дані досліджень нових ліків від масових хвороб, зокрема малярії. Головною задачею системи є вирахування ймовірності входу ліків в контакт з білками малярії [5];
4. Китайський проект China-Grid, який об'єднав комп'ютерні мережі найбільших китайських університетів.[6]

Grid-технології дозволяють вирішити проблеми, пов'язані з недоліком обчислювальних потужностей для наукових і виробничих задач, які потребують великого обсягу обчислень і/або обробки великих обсягів даних. Це досягається об'єднанням комп'ютерних ресурсів окремих наукових організацій, підприємств і компаній. Отримана в результаті мережа комп'ютерів використовується як єдиний ресурс.[5]

За нинішнього розвитку подібних систем є очевидним, що Grid стане новим важливим інструментом, який дозволяє великій кількості вчених набагато швидше виконувати трудомісткі розрахунки і справлятися із складними ресурсомісткими задачами.

Література

1. Концепция GRID [Електронний ресурс] – Режим доступу до ресурсу: https://sites.google.com/site/gridnach/koncepcia-grid.
2. Евгений Ивашко. (06.10.2009). *Распределенные вычисления: Часть 1. Высокопроизводительные вычисления в каждый дом.* Available: https://www.ibm.com/developerworks/ru/library/l-grid/. Lastaccessed 16.03.2016.
3. Grid Computing — новая парадигма Internet-вычислений [Електронний ресурс]. – 2001. – Режим доступу до ресурсу: http://itc.ua/articles/grid_computing_-_novaya_paradigma_internet-vychislenij_7249.
4. Как начать работать в грид. Пользовательский сценарий работы в грид. [Електронний ресурс], http://horst-7.bitp.kiev.ua/files/Lecture_2_ How_To_Work_Grid_v1.pdf.
5. А.П. Демичев. Введение в грид-технологии / А.П. Демичев, В.А. Ильин, А.П. Крюков – Москва: Препринт НИИЯФ МГУ, 2007. – С. 67-68, 71-72, 76
6. Грід [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Ґрід.

УДК 621.396.946

ЗАХИЩЕНІ БЕЗПРОВОДОВІ МОБІЛЬНІ СЕНСОРНІ МЕРЕЖІ ДЛЯ МОНІТОРИНГУ ПАРАМЕТРІВ НАВКОЛИШНЬОГО СЕРЕДОВИЩА

Давидюк В.О., Дакаєв О.В., Димид М.Д.
Інститут телекомунікаційних систем НТУУ «КПІ»
E-mail: va.davidyuk@gmail.com, sandak94@gmail.com, mariana.dymyd@gmail.com

Secured Wireless Network with Mobile Sensors for Environmental Monitoring

In this paper technical solutions are proposed for creating secured wireless networks and sensors for environmental monitoring of urban area as well as remote contaminated area.

У наш час з кожним роком швидкодія обчислювальної техніки зростає у кілька разів. Саме завдяки цьому з'являється велика кількість досить малих, але високопродуктивних мікроконтролерів (наприклад Raspberry Pi Zero, Arduino Nano тощо). Ці пристрої надають унікальну можливість щодо розподілення обчислювальної потужності між вузлами мережі. Крім цього, можливо створювати значний функціонал для окремих вузлів зі своєю операційною системою та застосунками, що дозволяє розбудовувати широкомасштабні розподілені безпроводові сенсорні мережі для моніторингу середовища [1]. Але при цьому залишається відкритим питання безпеки та мультисервісності у таких мережах.

У даній статті запропоновано модель, яка використовує ідею інтернету речей та представляє собою зразок розподіленої сенсорної мережі для моніторингу міської зони (CO2, забруднення повітря, пожежі, шум, рівень електромагнітного поля та ін.). Дані моніторингу збираються з вузлів, що можуть розташовуватись на автомобілях, автобусах, дронах тощо, та передаються через безпроводові мережі (GSM, 3G, Wi-Fi чи ZigBee) на віддалений сервер для подальшого опрацювання та візуалізації в режимі реального часу у web-додатку. Усі канали використовують VPN-з'єднання, що забезпечує розподіленість та безпеку мережі [2].

Одною з найбільших проблем безпроводових сенсорних мереж є безпека даних. Для вирішення даного питання ми пропонуємо використання VPN. Це рішення гарантує не тільки високий рівень безпеки, а також надає чудовий метод з'єднання елементів мережі. Зразок такої розподіленої мережі показано на рис. 1.

Існує 4 основні елементи, які в сумі дають високопродуктивну розподілену безпроводову сенсорну мережу.

1. Вузли. Кожен вузол містить материнську плату, сенсори, безпроводовий інтерфейс та джерело живлення. Ми пропонуємо використання мікроконтролерів у якості материнських плат, адже вони достатньо продуктивні для використання VPN та запуску додатків [2]. Для моніторингу середовища

існують сенсори що моніторять параметри (CO, забруднення повітря, пожежі, шум, рівень електромагнітного поля та ін.). В якості безпроводового інтерфейсу використаємо будь-яку доступну мережу (GSM, Wi-Fi або ZigBee). У запропонованій моделі вузли матимуть власні автономні джерела живлення.

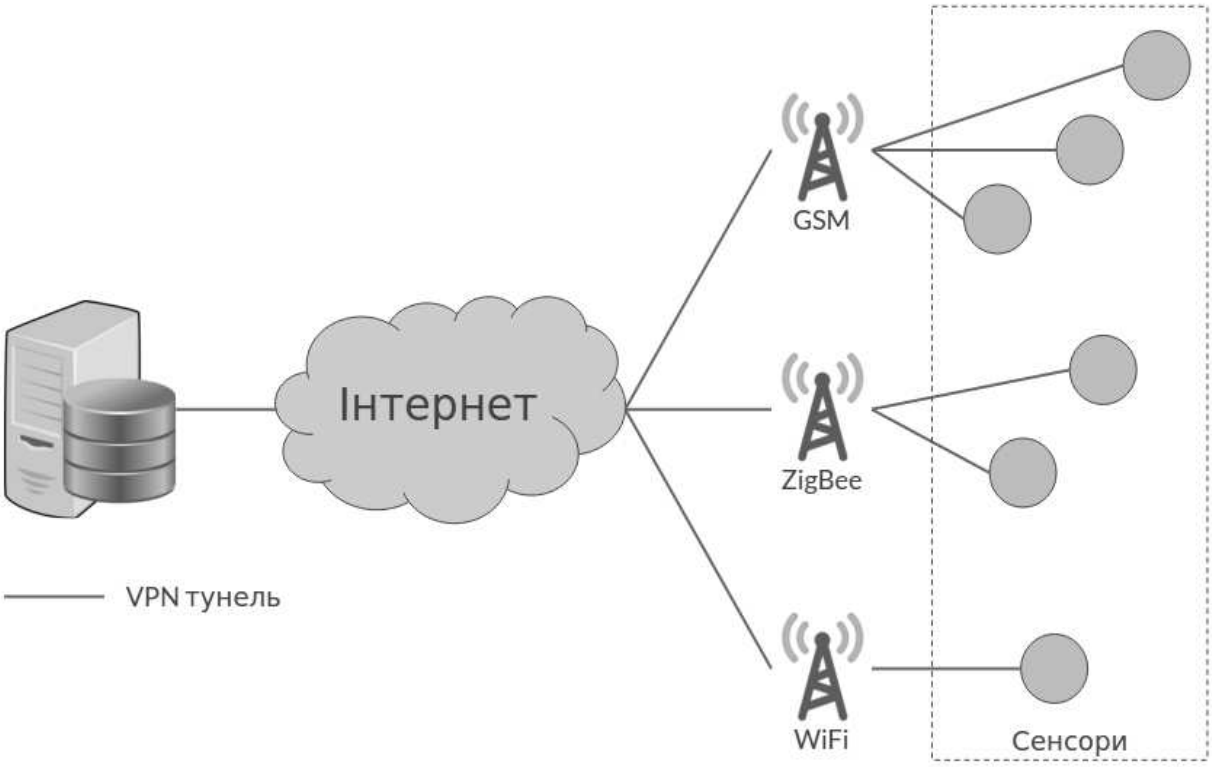


Рис. 1. Архітектура системи.

2. Мережевий інтерфейс. У нашому випадку, є досить великий вибір технологій. Якщо не буде використовуватись автономне джерело живлення, можливе застосування WiFi, UMTS та інших енергозатратних безпроводових рішень. Використання нової концепції 'ZigBee-over-IP' досить сильно спрощує використання VPN у мережах ZigBee.

3. VPN-з’єднання. Для того, щоб з’єднати вузли в мережу та гарантувати високий рівень безпеки даних, пропонується використовувати VPN. Кожен вузол використовує свій радіоінтерфейс для підключення до VPN-сервера. Після встановлення з’єднання, усі дані від вузла до сервера шифруються та передаються через VPN-тунель, перед цим енкапсульовані у спеціальні пакети. Даний метод є дуже простим та ефективним для побудови незалежної розподіленої мережі, адже після усіх виконаних дій ми отримуємо повноцінну мережу, подібну до локальної по характеристикам та функціоналу. Більше того, крім передачі даних з сенсорів через мережу є можливість транслювати потокове аудіо або відео. Наш VPN-сервер використовує протокол GRE через UDP-порт для кожного клієнта (вузла) для маршрутизації даних між елементами мережі.

4. Сервер. Саме він є найважливішим елементом мережі. Ми використовуємо кілька додатків на сервері. Перший – VPN-сервер, який необхідний для з’єднання розподілених вузлів. Другий важливий додаток – сервер баз даних – необхідно використовувати високопродуктивну базу даних

для великомасштабної мережі та великих потоків даних. Для хорошої сумісності рекомендується використовувати веб-додатки, отже стає необхідною наявність HTTP/HTTPS-серверу для нашої системи. Для динамічної генерації веб-сторінок можливо застосувати будь-яку поширену мову програмування, наприклад PHP або Ruby.

Однією з сучасних тенденцій у телекомунікаційних системах є використання безпілотних літаючих апаратів (БПЛА), які підтримуються нашей мережею [3]. Є можливість приєднати вузол до БПЛА та збирати дані у різних географічних зонах. За допомогою сенсора GPS відкривається можливість додавати геотеги до зібраних даних, за допомогою яких створювати потужні системи моніторингу з застосуванням інтерактивних карт. Наприклад, після пожежі на певному об'єкті доцільно використовувати БПЛА з сенсорами забруднення повітря, після чого створити інтерактивну карту, на якій можна буде побачити актуальні рівні забруднення по території, отже населення зможе вжити певних заходів, наприклад покинути територію або закрити вікна.

Таким чином, для розв'язання проблеми з безпекою доцільно застосовувати VPN – з'єднання. Крім цього, для енергоефективного і компактного рішення пропонується побудова мережі на основі модулів XBee. Для безпечного розміщення вузлів у зонах аварій чи лиха можливе використання БПЛА [3]. У міській зоні є змога використовувати більш складні сенсори з використанням зовнішніх процесорів, а також модулів Wi-Fi або 3G.

У даній статті розглянута досить проста, проте потужна ідея побудови розподіленої безпроводової мобільної сенсорної мережі для моніторингу параметрів навколишнього середовища. Запропонована система має значні переваги у безпеці даних, простоті побудови та простоті управління. В подальшому, система матиме значний потенціал щодо модернізації та впровадження новітніх розробок, зокрема, нових систем автоматизації різноманітних процесів та нових систем моніторингу, обліку та візуалізації даних. Ці питання будуть надалі розв'язуватись та розглядатимуться у подальших публікаціях.

Література

1. Лисенко О.І., Нікулін О.Ф., Чумаченко С.М., Валуйський С.В. Задача оптимального розміщення сенсорів. Технології екологічного моніторингу із використанням інтелектуальної сенсорної техніки // Проблеми телекомунікацій: 8-а Міжнар. наук.-техн. конф., 22-25 квіт. 2014р. : матеріали конф. – К., 2014. – С. 53-56.
2. P. Likhar, R. S. Yadav, and K. Rao M, "Securing IEEE 802.11G WLAN Using OpenVPN and Its Impact Analysis," International Journal of Network Security & Its Applications (IJNSA), 2011, vol. 3, №6, pp. 97-113.
3. S. Valuiskyi, O. Lysenko, T. Pryshchepa, and S. Chumachenko "The problem of finding a rational topology of wireless sensor networks using UAVs," 2nd Int. IEEE Conf. PIC S&T, Ukraine, Kharkiv, 13-15 Oct., 2015, vol. 1, pp. 213-215.

УДК 621.396

ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ПРОПУСКНОЇ ЗДАТНОСТІ БЕЗПРОВОДОВОЇ СЕНСОРНОЇ МЕРЕЖІ

Давидюк В.О., Петрова В.М.
Інститут телекомунікаційних систем НТУУ «КПІ»,Україна
E-mail: va.davidyuk@gmail.com

Providing of throughput stability in wireless sensor network

In this article an idea of maximum efficiency MAC protocol is proposed for using in wireless sensor networks with probability of increasing of nodes quantity. A research of optimal delay time window is provided in order to avoid throughput degradation during increasing of network size.

З впровадженням малопотужних безпроводових сенсорних мереж у різних галузях науки та техніки, дослідження можливості їх масштабування стає головним критерієм при розробці ефективних протоколів медіадоступу. У мережах значних розмірів, що складаються з вузлів, які можуть одночасно входити у режими високої активності при виникненні певних впливаючих факторів, пропускна здатність цих мереж може значним чином зменшуватись у той час, коли велика кількість вузлів починає передавати дані. Більше того, при зростанні вимог по передачі даних, буде зростати необхідна кількість вузлів мережі, що буде ускладнювати і без того існуючу проблему. Отже, при розробці протоколів медіадоступу необхідно враховувати у якості одного з головних критеріїв залежність пропускної здатності від кількості вузлів, що приймають участь при передачі.

Алгоритм CSMA/CA, котрий включений у специфікацію MAC у IEEE 802.15.4, підтримує безпроводові ad-hoc мережі з низькою потужністю та невисокою пропускною здатністю, що складаються з сенсорів, та можуть сягати розмірів 255 вузлів. У CSMA/CA дуже широко використовується алгоритм BEB (binary exponential back off, двійкова експоненційна затримка). У BEB, кожна станція обирає випадковий таймер, що рівномірно розподілений всередині певного часового інтервалу, так званого «вікна». Таймер затримки починає відраховувати час тоді, коли канал залишається не використовуваним більше часу ніж розподілений інтервал між кадрами DIFS (distributed inter frame space), зупиняється відповідно тоді, коли починається передача. Коли таймер дораховує час до нуля, вмикається передача свого тайм-слота. У випадку виявлення колізій, часове вікно збільшується вдвічі, але не більше певного значення CW_{max}. При вдалій передачі, вікно зменшується до свого мінімального значення CW_{min}.

В інших джерелах було розглянуто проблему масштабування мереж шляхом зміни параметрів MAC, аби пристосуватись до зміни кількості вузлів. У даній статті продемонстрований підхід, спрямований на знаходження оптимальних розмірів часових вікон, аби мінімізувати вплив можливого зростання мережі на пропускну здатність. Варто зазначити, що у даній статті ми використовуємо визначені розміри вікон затримки $[W_1, W_2 \dots W_m]$.

Визначимо початкові умови. У нашій моделі час ділиться на слоти, довжина пакетів постійна, кожна рівна одному тайм-слоту. Припустимо, що усі вузли синхронізовано і передача починається з початком кожного слоту. Оскільки мережа є досить навантажена, у кожної станції є пакет для передачі і з ймовірністю τ станція передає пакет у даному слоті.

Припустимо, що ймовірність колізії незмінна, тобто кожна станція, що ініціює передачу, матиме колізію з постійною ймовірністю p. Дане припущення є швидше інтуїтивним, у тому сенсі, що з ростом кількості вузлів n, стан системи, тобто повна кількість пакетів, що потенційно будуть потрапляти у колізії з даною станцією, не буде залежати від кількості повторних передач даної станції. Маючи ймовірність передачі, можливо вивести таку величину, як фактор колізії:

$$c = \frac{p}{1-p} \quad . \tag{1}$$

Оскільки відношення між ймовірностями передачі та колізій виражається складними нелінійними рівняннями, розв'язання задачі для довільних розмірів вікна є дуже складним та у деяких випадках неможливим. Як показано на рис. 1, хоч відношення і нелінійне, якщо ми сформуємо функцію затримки (2) близькою до ідеальної ступінчатої функції, тоді результуючі розв'язання завжди будуть вести до точної ймовірності колізій[1], і якщо ця ймовірність близька до оптимальної, пропускна здатність буде оптимальною при різноманітних розмірах мережі.

Щоб зімітувати ідеальний метод затримки, використаємо методи апроксимації. Задача зводиться до знаходження значень розмірів вікон затримки W_i, щоб апроксимувати реальну функцію затримки з ідеальною [1] (рис. 1):

$$\tau_{seq} = \frac{2(1-c^{m+1})}{\sum_{i=0}^{m}(1-c)c^i W_i + 1 - c^{m+1}} \approx \tau^*(c) \tag{2}$$

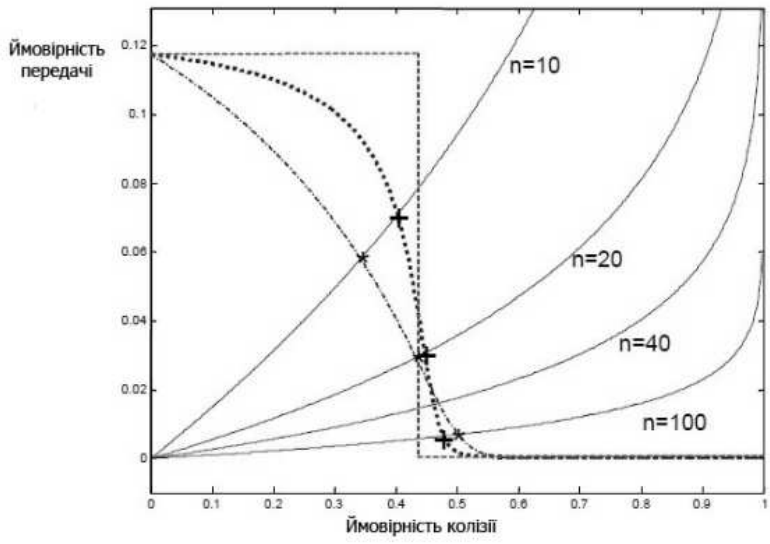


Рис. 1 Порівняння розглянутого алгоритму і двійкового експоненційного алгоритму затримки в залежності від кількості вузлів.

Апроксимація Баттерворта є найпростішою, в той час, коли еліптична апроксимація того самого порядку демонструє дещо кращий результат.

При використанні апроксимації Баттерворта *k*-го порядку отримано такі розміри вікон затримки:

$$W_i = \sum_{j=0}^{\lfloor i/k \rfloor} W_0 \left(\frac{1}{c}\right)^{k \cdot j} \qquad i \le m \tag{2}$$

Для наведеного нижче моделювання апроксимованої функції використовувались WLAN 802.11b модулі OPNET. Фізичний рівень базується на розширенні спектру зі скачкоподібним переналаштуванням частоти зі швидкістю передачі даних 1 Мбіт/с.

У першому випадку, кількість вузлів змінюється від 5 до 120, кожна станція передає пакети довжиною 1024 байти. Час між передачами обрано так, щоб черги передачі ніколи не залишались пустими. Результатом моделювання було отримання статистики пропускної здатності у стаціонарному стані системи. Результати показані на рис. 2

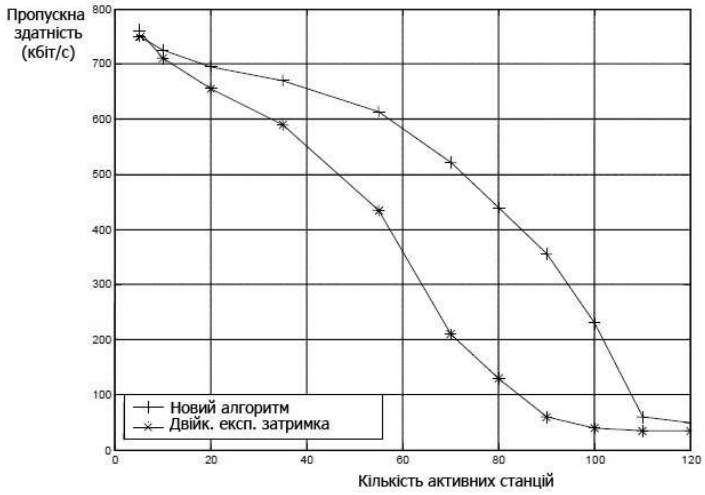


Рис. 2 Середня пропускна здатність при використанні розглянутого алгоритму і існуючого двійкового експоненційного алгоритму затримки.

У даній статті було розглянуто питання зменшення пропускної здатності у мережах adhoc зі зростанням розмірів мережі. Для розв'язання цієї проблеми було запропоновано альтернативний режим затримки, що використовує новий алгоритм. Було показано, що він демонструє високу пропускну здатність зі зростанням кількості вузлів мережі. Результати моделювання також довели це твердження.

Література

1. Ali Motamedi, Hamid Aghajan, Ahmad Bahai Throughput Persistence of Scalable Mobile Ad-hoc Networks: Evaluation and Enhancement, 2004.
2. G. Bianchi, I. Tinnirello “Kalman filter estimation of the number of competing terminal sin IEEE 802.11 network,” INFO COM 2003, 22(2) , 844 – 852, 2003.
3. Jian Ma, “IEEE 802.11 Distributed coordination function (DCF): Analysis and enhancement”, ICC 2002 - IEEE International Conference on Communications, no. 1, April 2002 pp. 605-609.4.

УДК 621.3

VHF і UHF АНТЕНА ДЛЯ НАНОСУПУТНИКА

Бендасюк Н., Прищепа Т.О.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: prischepa@i.ua, Bendasiuk@gmail.com

VHF & UHF Antena for nanosatellite

Today nanosatellite has become standard for universities and other research groups. NANOSATELLITE - the future of communication technology and a huge step forward in space exploration. One of the main components of the complex, while a new generation of spacecraft is their communication system.

На зміну великих Космічних апаратів приходить нове покоління супутників - легкі, економічні у витраті енергії, маленькі і високоманеврені апарати. Зазвичай їх поділяють на три категорії: мікросупутники, вагою від 10 до 100 кілограмів, наносупутники - від 1 до 10 кг і пікосупутники (менше одного кілограма). Часто зустрічаються в літературі супутники формату Cubesat, це є наносупутники із стандартизованим розміром (100 × 100 × 100 мм). На сьогоднішній день вони стали стандартом для ВУЗів, та інших дослідницьких груп. Наносупутники - майбутнє комунікаційних технологій і величезний крок вперед в дослідженні космосу. Одним з найголовніших і одночасно складних компонентів космічних апаратів нового покоління є їх система зв'язку [2].

Основною складовою є антена з жорсткими масо-габаритними характеристиками. З точки зору електромагнітної сумісності антен, необхідні багато-променеві направлені та ненапрямлені діаграми спрямованості. Ефективним рішенням для таких вимог є багатофункціональні антенні системи [2], що дозволяють одночасне використання в різних режимах випромінювання.

Нами була розроблена телекомунікаційна система PolyITAN-1, яка має два види передачі даних. Це радіомаяк (20,8 дБм або 120 мВт, 10 біт/с в азбуці Морзе на 437 МГц) який функціонує постійно, який по команді із наземної станції перемикається в режим зв’язку з FSK модуляцією на швидкості 9600 біт/с та вихідною потужністю 30дБм dBm (1Вт) на частоті 437 МГц. Сигнал висхідній лінії зв'язку використовує 145 МГц несучої частоти з модуляцією AFSK та швидкістю передачі 1200 біт/с.

Елементами антен використовуються бронзові смужки (вібратори) зображені на рис.1, з довжиною 570 мм для приймального діапазону 144 МГц та 175 мм для робочого діапазону частот 435 МГц. Для придання бронзовим смужкам пружних властивостей, вони проходять термічну обробку

Рис. 1 Зовнішній вигляд бронзових смужок.

Так як конфігурація PolyITAN-1 відноситься до формату Cubesat [1], то габарити не повинні перевищувати 100 × 100 мм на стороні, тому для двох антен, що використовується для зв'язку з наземними станціями, використовується система розгортання антен. На Рис.2 показаний зовнішній вигляд антенної системи у згорнутому вигляді, габарити якої складають 100 × 100 × 8 мм.

Передбачається механізм розкриття вібраторів після виводу супутника у відкритий космос. Механізм розкриття антен представлений на рис. 3, реалізований переплавленням капронової нитки діаметром 0,15 мм на нагріваючому елементі, що керується центральним процесором наносупутника.

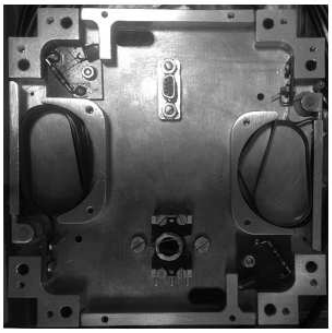


Рис. 2 Зовнішній вигляд двох діапазонної антени (144 МГц та 435 МГц) наносупутника при згорнутих вібраторах.

Рис. 3 нагріваючий елемент з капроновою ниткою .

Нагріваючий елемент представляє собою ніхромовий провід діаметром 0,2мм. та питомим опором 2,8 Ом, що намотаний на циліндричний корпус діаметром 2мм та довжиною 8мм. Після виходу супутника з контейнеру через 30хв. на нагріваючий елемент подається напруга з батарей 3,3 В на 10 секунд температура на якому підіймається до 190ºС та переплавляє капронову нитку. І антена під дією пружинок та пружинних властивостей, приймає форму штиря.

Характеристика коефіцієнту відбиття (Рис. 4) показує, що антени добре узгоджена в діапазоні частот 435 МГц. Розраховані діаграми направленості випромінювання дещо відрізняються від діаграми направленості класичного несиметричного вібратора. На Рис. 5 наведені діаграми направленості антен в площинах H та E відповідно. Так на Рис. 4 видно спотворення діаграми в обох площинах: немає ідеального кола в H-площині та ідеальної вісімки в E-площині. Спотворення зумовлені близьким розташуванням антенних вібраторних елементів один до одного, а також малими габаритами самого наносупутника по відношенню до довжини хвилі. Вказані спотворення не

вплинуть негативно на якість зв’язку.

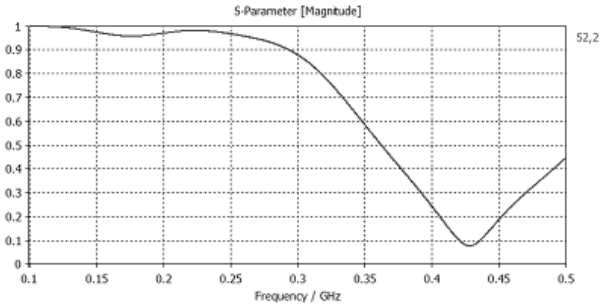


Рис. 4. Характеристика коефіцієнту відбиття антен, налаштованих на діапазон частот 435МГц.

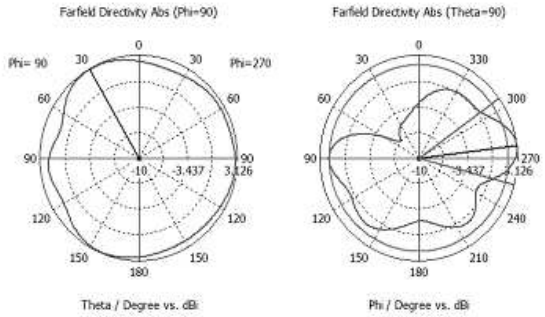


Рис. 5. Діаграми направленості в Н-площині (зліва) та Е-площині (справа) випромінювача 435 МГц

В діапазоні 144 МГц характеристики вібраторних антен ближчі до ідеальних і показані на Рис. 6.

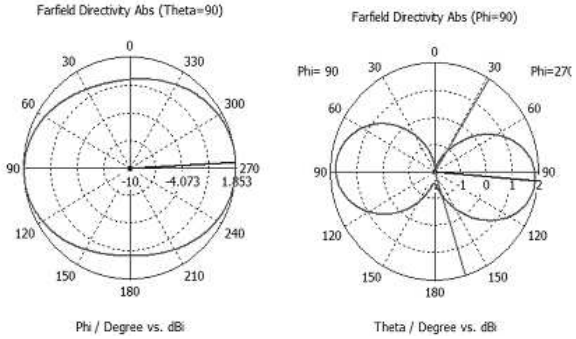


Рис. 6. Діаграми направленості в Н-площині (ліворуч) та Е-площині (праворуч) випромінювача 144 МГц

Література

1. Биндель Д., Овчинников М.Ю., Селиванов А.С. и др. Наноспутник GRESAT. Общее описание / Препринт ИПМ им. М.В. Келдыша РАН. — М., 2009. — 35 с.
2. Камнев В. Е. Спутниковые сети связи: учеб. пособие / В. Е. Камнев, В. В. Черкасов, Г. В. Чечин. – М.: Альпина Паблишер, 2004. – 536 с.

УДК 621.3

АНАЛІЗ ЕНЕРГОСПОЖИВАННЯ ВУЗЛА БЕЗПРОВОДОВОЇ СЕНСОРНОЇ МЕРЕЖІ

Бондарук О.А., Петрова В.М.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: alex.bondaruk9@gmail.com

Energy consumption analysis of wireless sensor network node

The article outlines the problem of power consumption and energy efficiency nodes of wireless sensor networks (WSN). The main factor influencing the increase in the likelihood of disruption of the sensor network is a limited resource supply node. There is presented method of calculating the energy consumption of node and the lifetimeof the powerelements.

Розглянута проблема енергоспоживання і підвищення енергоефективності вузлівбездротових сенсорних мереж (БСМ). Виявлено, що основним фактором, що впливає на збільшенняймовірності порушення роботи сенсорної мережі є обмеженість ресурсу енергоживлення вузла. Наведено методику розрахунку енергоспоживання вузлів і терміну служби елементів їх живлення.

За минуле десятиліття широке поширення набули бездротові мережі зв'язку.При вирішенні багатьохзадач, пов'язаних з промисловим моніторингом,побудовою системи «Розумний будинок», системирозподіленого збору інформації та іншими,актуальними стають мережі з передачеюінформації до 1 Мбіт / с. Дотаких мереж відносять і бездротові сенсорні мережі.При проектуванні і реалізаціїбездротових сенсорних мереж необхідно вирішитибезліч складних проблем, одною зосновних проблем є забезпечення високої енергоефективності, адже датчики що використовуються в БСМ зазвичай мають автономну систему живлення. Отже, підвищенняенергоефективності вузлів безпровідних сенсорних мереж є актуальною темою длядосліджень, а аналіз енергоспоживанняі оптимізація - перспективним напрямомне тільки в БСМ, але і в багатьох іншихбездротових мережах.

Одним з головних вимог до БСС єїх автономність, забезпечити яку можна,зменшивши енергоспоживання кожного вузла.Для вирішення даної проблеми використовуютьнаступні методи:

- визначення і оптимізація часувключення передачі;
- багатовузлова передача, тобто відправка повідомлень через проміжні вузли замістьпрямої дальньої передачі;
- попередня обробка та скороченняобсягу даних, необхідних для передачі.

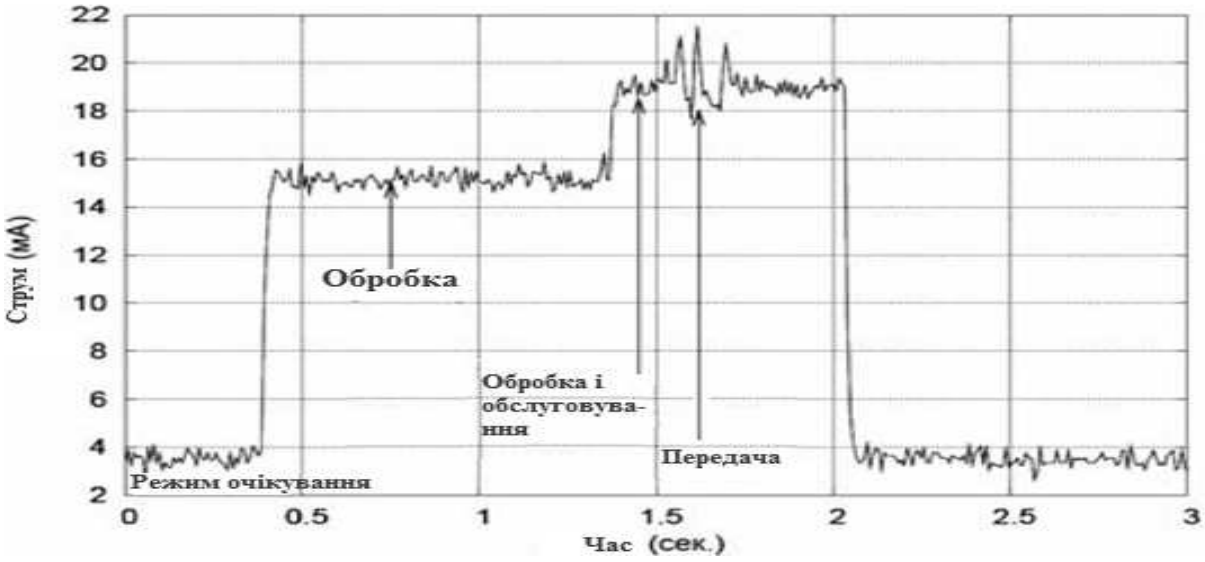


Рис.1. Приклад осцилограми споживання струму
сенсорним вузлом в залежності від фази обробки запиту

Щоб однозначно відповісти, які режимироботи потрібно звести до мінімуму, розглянемо номінальне енергоспоживання трансівераCC2530, який представляє собою приймальнопередавач і мікроконтролер (ядро MCS-51) наодному кристалі, табл. 1.

Таблиця 1. Номінальне енергоспоживання трансівера CC2530 в різних режимах

Тип режиму роботи	*Прослухову-вання ефіру(Mode RX)*	*Відправка повідомлень(ModeTX на 1dBm)*	*Робота мікро-контролера*	*Режим пробудження (протягом 4мкс)*	*Режим сну*
Спожи-вання	24	29	9	0,2	Від 0,0004 до 0,001

Енергоспоживання вузла E за один цикл,виходячи з проведеного аналізу, можна визначитияк суму енергій споживання:

$$E_e = E_{slep} + E_{MCU} + E_{rcv} + E_{trans} + E_{other} \quad (1)$$

де E_{slep} - енергія, споживана вузлом в фазі сну;E_{MCU} - енергія, споживана вузлом під час роботи мікроконтролера або обчислювального ядра приймача при його відсутності; E_{rcv} - енергія, споживана вузлом під час прийому; E_{trans}- енергія, споживана вузлом під час передачі;E_{other} - енергія, споживана вузлом в іншихрежимах (режим пробудження і ін.)

Висновки. Енергоспоживання - ключовий параметр якості роботи БСС, тому питання про його розрахункупри створенні подібних систем виникає одним зперших. У статті проведено аналіз енергоспоживаннявузла безпровідної сенсорної мережі.Механізми зменшення споживання енергіївузлом БСС залежать від моделі збору інформації.Також на споживання енергії вузла впливає алгоритмроботи вузла, побудований за моделлю зборуінформації.Величина енергоспоживання залежить відбезлічі факторів, тому, для того щобоцінити час життя мережі, використовують моделі енергоспоживання, здатні реалістично описати споживання мережі.

Література

1. Терентьев, М. Н. Метод функционирования систем мониторинга параметров объектов с изменяемой конфигурацией на базедискретных беспроводных сенсорних сетей [Текст]: дис. … к. т. н.: 05.13.15 /М. Н. Терентьев. – М., 2010.– 154 с.
2. Иванова, И. А. Определение периметра зоны покрытия беспроводных сенсорних сетей [Текст] /И. А. Иванова // Промышленные АСУ и контроллеры. –2010. – № 10. – С. 25–30.
3. Measuring Power Consumptionof CC2530 WithZStack [Electronicresource] / Texas Instruments Application Ноте AN079. – Availableat:http://www.ti.com/lit/an/swra292/swra292.pdf/ – 10.06.2014 г.– Titlefronthescreen.
4. Власова, В. А. Анализ энергоцикловузловбеспроводныхсенсорныхсетей [Текст] / В. А. Власова, А.Н. Зеленин // Восточно-Европейский журнал передовыхтехнологий. – 2012. – Т. 3, № 9 (57). – С. 13–17.
5. SecondGenerationSystem-on-ChipSolutionfor 2.4GHz IEEE 802.15.4 / RF4CE / ZigBee [Electronicresource] /TexasInstruments. – Availableat:http://www.ti.com/lit/ds/symlink/cc2530.pdf/ – 15.06.2014. – Titlefromthescreen.
6. IEEE Standard forInformationTechnology –TelecommunicationsandInformation Exchange BetweenSystems – LocalandMetropolitanAreaNetworks – SpecificRequirements – Part 15.4: WirelessMedium Access Control(MAC) andPhysicalLayer (PHY) SpecificationsforLow-RateWirelessPersonalAreaNetworks (WPANs) [Electronicresource] / IEEE Std. 802.15.4-2009. – Availableat:http://standards.ieee.org/getieee802/download/802.15.4d-2009.pdf/ –11.06.2014. – Titlefromthescreen.

УДК 621.39

МЕТАМАТЕРИАЛЫ И СВЯЗАННЫЕ С НИМИ ПРОЦЕССЫ

Живков А.П., Студенюк Р. Ю.
Физико-технический институт НТУУ НТУУ «КПИ», Украина
E-mail: zhivkovalex@gmail.com

Metamaterials and related processes

Several processes deal with metamaterials were studied. Future SHF- and teracycle-technologies will be based on metamaterials. Quite possibly, metamaterials will lay the foundation of new technologies in this frequency bands.

В материалах с отрицательным показателем преломления фазовая и групповые скорости разнонаправлены, при чем принято считать, что фазовая скорость является отрицательной, а групповая – положительной [1].

Некоторые авторы [1] в своих статьях, основываясь на разнонаправленности фазовых и групповых скоростей, утверждали, что одним из примеров проявления метапроцесса является эффект Доплера. Нередко этот эффект наблюдается в акустике - если источник звука направляется к наблюдателю, то частота звука повышается, если же источник движется в противоположную сторону, частота звука понижается (рис.1). Знак доплеровского сдвига частоты будет определяться знаком коэффициента преломления [2], это зависит от направленности групповой и фазовых скоростей и является признаком метаматериальности (рис.2).

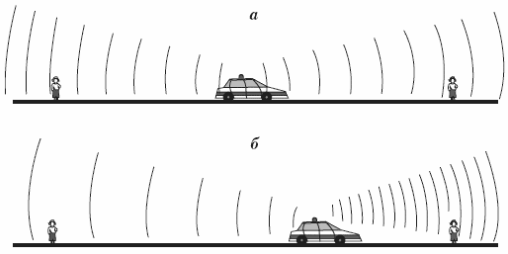


Рис.1 Пример доплеровского смещения в акустике.

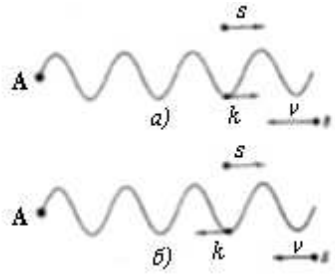


Рис. 2 Метаматериальность в эффекте Доплера: а) n>0; б)n<0, при этом: A –источник излучения; B –приемник; S –вектор Пойтинга; k –волновой вектор.

Причиной «красного смещения» в астрономии также является эффект Доплера [3], что так же можно отнести к эффекту метатериальности, так как направление движение источника (групповая скорость) и направление излучения (фазовая скорость) противоположны (рис. 3).

Рис. 3 «Красное смещение».

Если в некоторой среде движется заряженная частица с релятивисткой скоростью, большей скорости света в этой среде, наблюдается излучение Вавилова-Черенкова, который является сложным эффектом Доплера [4].

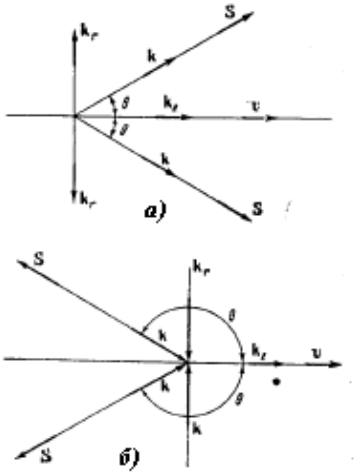


Рис. 4 Эффект Вавилова-Черенкова: а) n>0, б) n<0

Некоторые авторы [5] относят к метапроцессам и мираж (рис. 5). Задолго до появления понятия «метаматериал» мираж был детально описан в классическом курсе физики Фейнмана [6] (рис.6)

Рис. 5 «Летучий Голландец».

Рис. 6 «Мираж» (из курса ФЛФ).

Эти эффекты образованы так называемыми градиентными метаматериалами. Вполне вероятно (однако авторам пока не удалось найти в литературе подтверждения этой гипотезе), что к этому же классу явлений можно отнести и преломление радиоволн определенной длины в тропосфере (рис. 7), описанное в [7], где отмечается, что «отражения от слоистых неоднородностей в тропосфере являются одной из основных причин дальнего тропосферного распространения УКВ».

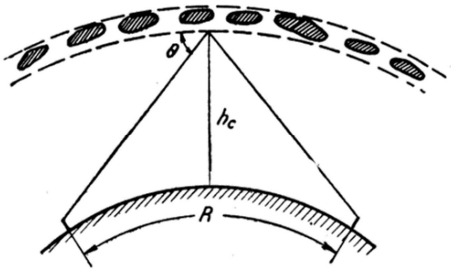


Рис. 7. Отражению радиоволн от приподнятого турбулентного слоя.

Стробоскопический эффект так же обладает особенность разнонаправленности групповой и фазовых скоростей, которая проявляется в эксперименте с вращающимся колесом (пропеллером, диском), освещенным мигающим источником света. В этом процессе задействованы колебания различного типа, а так же разной природы – механические (вращающийся диск) и оптические (мигающий источник света). Диск (ротатор) вращается с частотой f_1, частота вспышек (осциллятор) - f_2. Наблюдаемое движение отдельной «спицы» на диске можно интерпретировать как фазовую скорость. На рис.8 представлены варианты наблюдаемого вращения спицы в зависимости от соотношения частот вращения диска и вспышек.

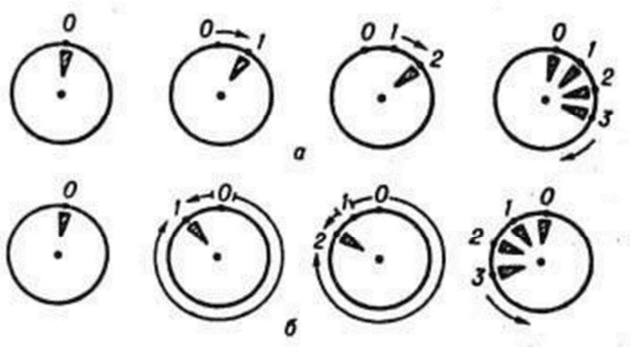


Рис. 8 Явление строб-эффекта: а) $f_1 > f_2$, вращение по часовой стрелке б) $f_1 < f_2$, вращение против часовой стрелки, диск вращается по часовой стрелке.

Таким образом, в рассматриваемом процессе $f_1 < f_2$ (частота ротатора больше частоты осциллятора), как и в метаматериалах. Поэтому вполне правомерно назвать рассматриваемый вариант стробоскопического эффекта «метапроцессом».

Литература

1. В. Г. Веселаго, Волны в метаматериалах: их роль в современной физике, УФН, 2011, том 181, номер 11, 1201–1205.
2. В. Г. Веселаго, Метаматериалы и их роль в современной физике, УФН, 181, вып.11, 11.10.2011, с. 15-16,86.
3. «Красное смещение», Новости науки и техники: http://femto.com.ua/articles/part_1/1806.html.
4. Зрелов В. П., Излучение Вавилова - Черенкова и его применение в физике высоких энергий, т. 1 - 2, М., 1968.
5. Tutorials in Metamaterials /Mikhail A. Noginov, Viktor A. PodolskiyOctober 25, 2011 by CRC Press - 308 Pages
6. «Optics: The Principle of Least Time», Michael A. Gottlieb, and Rudolf Pfeiffer http://feynmanlectures.caltech.edu/I_26.html.
7. Давыденко Ю.И. Дальняя тропосферная связь. М., Военное издательство. – 212 с.

УДК 621.396.96

РЕКУРРЕНТНЫЙ АЛГОРИТМ ПАССИВНОЙ ЛОКАЦИИ В СЕНСОРНОЙ СЕТИ ПО РАЗНОСТНО-ДАЛЬНОМЕРНОМУ МЕТОДУ ПРИ НЕКОРРЕЛИРОВАННЫХ ОШИБКАХ ИЗМЕРЕНИЙ

Товкач И.О., Жук С.Я.
Радиотехнический факультет НТУУ «КПИ», м. Киев, Украина
E-mail: tovkach.igor@gmail.com

Recursive algorithm of the passive location in sensor networks based on the *time difference of arrival* method in case of uncorrelated errors of measurements

Using the mathematical apparatus of Kalman filtering is developed quasi-optimal recursive algorithm for determining the coordinates of the radio source in sensor networks based on the *time difference of arrival* method. Using statistical modeling is analyzed of the accuracy characteristics of the algorithm and compared with the Cramer-Rao lower bound.

Задача пассивного определения местоположения источников радиоизлучения (ИРИ) находит широкое применение при мониторинге окружающего пространства, ликвидации последствий стихийных бедствий, в интеллектуальных транспортных и охранных системах. В настоящее время для ее решения применяются сенсорные сети. При определении координат ИРИ на плоскости сенсорная сеть должна состоять из трех или более датчиков (Д).

Один из основных подходов пассивного определения местоположения ИРИ основывается на применении разностно-дальномерного метода (РДМ), в котором используются разности задержек между сигналами, полученными различными датчиками. Данный метод имеет существенное преимущество в простоте реализации, так как не требует синхронизации между ИРИ и датчиками сети и находит широкое применение на практике.

В известных методах определения местоположения ИРИ на основе РДМ [1], вычисление координат выполняется после поступления измерений от всех датчиков. В работе на основе математического аппарата калмановской фильтрации разработан квазиоптимальный алгоритм, который после формирования начальных условий на основе измерений времени прихода сигналов от четырех датчиков, позволяет рекуррентно уточнять местоположение ИРИ по мере поступления измерений от остальных датчиков.

На рис. 1 показана структурная схема сенсорной сети на плоскости, состоящей из девяти датчиков с координатами $\left(x_i^{Д}, y_i^{Д}\right)$, $i=\overline{0,8}$. Положение ИРИ характеризуется точкой с координатами (x,y). Уравнения РДМ для сети, включающей $n+1$ датчиков, имеют вид

$$d_{i0} = R_i - R_0 + v_i,\ i=\overline{1,n}, \qquad (1)$$

где R_i – расстояние между i – м датчиком и ИРИ $i=\overline{1,n}$; R_0 – расстояние между опорным датчиком и ИРИ; d_{i0} разность расстояний между R_i и R_0 $i=\overline{1,n}$; v_i –

некоррелированная погрешность измерения [1] с дисперсией $\sigma_v^2 \;\; i=\overline{1,n}$.

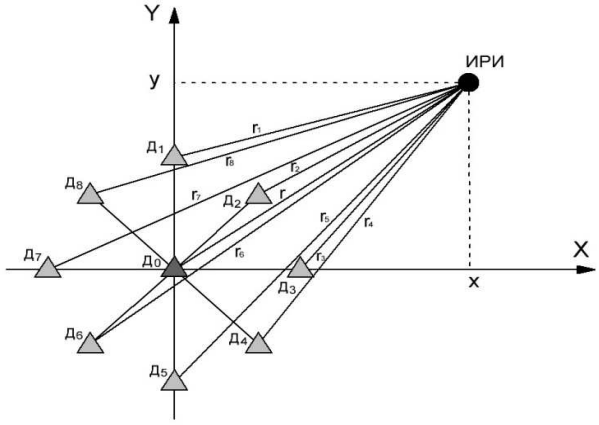


Рис. 1.

Полагается, что за время измерения разности дальностей между ИРИ и датчиками сети, его координаты не меняются, поэтому уравнение, описывающее динамику изменения координат положения ИРИ, имеет вид

$$u_k = u_{k-1}, \tag{2}$$

где $u_k = \left(x_k, y_k\right)^T$ – вектор состояния, включающий координаты положения ИРИ на текущем такте *k*.

Уравнение измерения с учётом (1) можно представить в виде

$$r_k = h(u_k) + v_k, \tag{3}$$

где $h(u_k)$ – нелинейная функция, которая описывается выражением

$$h(u_k) = \sqrt{(x_k - x_k^{Д})^2 + (y_k - y_k^{Д})^2} - \sqrt{x_k^2 + y_k^2}\,.$$

Уравнение измерения (3) является нелинейным.

С использованием модели (2), (3), квазиоптимальный алгоритм оценивания координат ИРИ может быть получен на основе расширенного фильтра Калмана [2] и описывается уравнениями

$$K_k = \hat{P}_{k-1} \cdot \frac{\partial h^T(\hat{u}_{k-1})}{\partial u_k} \left[\frac{\partial h(\hat{u}_{k-1})}{\partial u_k} \hat{P}_{k-1} \frac{\partial h^T(\hat{u}_{k-1})}{\partial u_k} + \sigma^2 \right]^{-1}; \tag{4}$$

$$\hat{u}_k = \hat{u}_{k-1} + K_k \left[r_k - h(\hat{u}_{k-1}) \right]; \tag{5}$$

$$\hat{P}_k = \hat{P}_{k-1} - K_k \frac{\partial h(\hat{u}_{k-1})}{\partial u_k} \hat{P}_{k-1}, \tag{6}$$

где $\hat{u}_k$ – оценка вектора состояния u_k; $\hat{P}_k$ – корреляционная матрица ошибки оценки вектора состояния u_k; K_k – коэффициент усиления фильтра;

$$\frac{\partial h(\hat{u}_{k-1})}{\partial u_k} = \left[\frac{\hat{x}_{k-1} - x_k^{Д}}{R_k^*} - \frac{\hat{x}_{k-1}}{R_{0k}^*}; \frac{\hat{y}_{k-1} - y_k^{Д}}{R_k^*} - \frac{\hat{y}_{k-1}}{R_{0k}^*} \right]; R_k^* = \sqrt{(\hat{x}_{k-1} - x_k^{Д})^2 + (\hat{y}_{k-1} - y_k^{Д})^2}\;;$$

$R_{0k}^* = \sqrt{\hat{x}_{k-1}^2 + \hat{y}_{k-1}^2}$.

Для выполнения калмановской фильтрации необходимо задать начальные условия. Начальная оценка вектора состояния $\hat{u}_0$ определяется на основе метода наименьших квадратов при наличии трех измерений разностей дальностей [3]. Начальная корреляционная матрица $\hat{P}_0$ определяется с использованием метода

квадратичной коррекции [1].

Моделирование алгоритма на основе РДМ проведено для конфигурации сенсорной сети рис. 1, где Д0 $(0;0)$, Д1 $(0;20)$, Д2 $(20\sqrt{2};20\sqrt{2})$, Д3 $(20;0)$, Д4 $(20\sqrt{2};-20\sqrt{2})$, Д5 $(0;-20)$, Д6 $(-20\sqrt{2};-20\sqrt{2})$, Д7 $(-20;0)$, Д8 $(-20\sqrt{2};20\sqrt{2})$. ИРИ располагается на окружности с радиусом 100 км. относительно опорного датчика Д0. Погрешность измерения датчиков $\sigma = 30$ м. В качестве показателя эффективности использовалось круговое СКО $\widehat{\sigma} = \sqrt{tr(\widehat{P})}$.

Фактическое круговое СКО $\hat{\sigma}^{MK}$ (кривая 1) ошибки оценки местоположения ИРИ, полученное методом Монте-Карло, а также теоретическое СКО $\hat{\sigma}$ (кривая 2), которое получено аналитически, показаны на рис. 2. Значение фактического СКО колеблется относительно его теоретического. СКО $\hat{\sigma}^{MK}$ принимает значения в пределах от 0.65 до 1.08 км. Также на рис. 2 (кривая 3) показано СКО $\hat{\sigma}_{НГРК}$, которое соответствует нижней границе Рао-Крамера (НГРК), которая характеризует потенциальную возможную точность определения координат ИРИ.

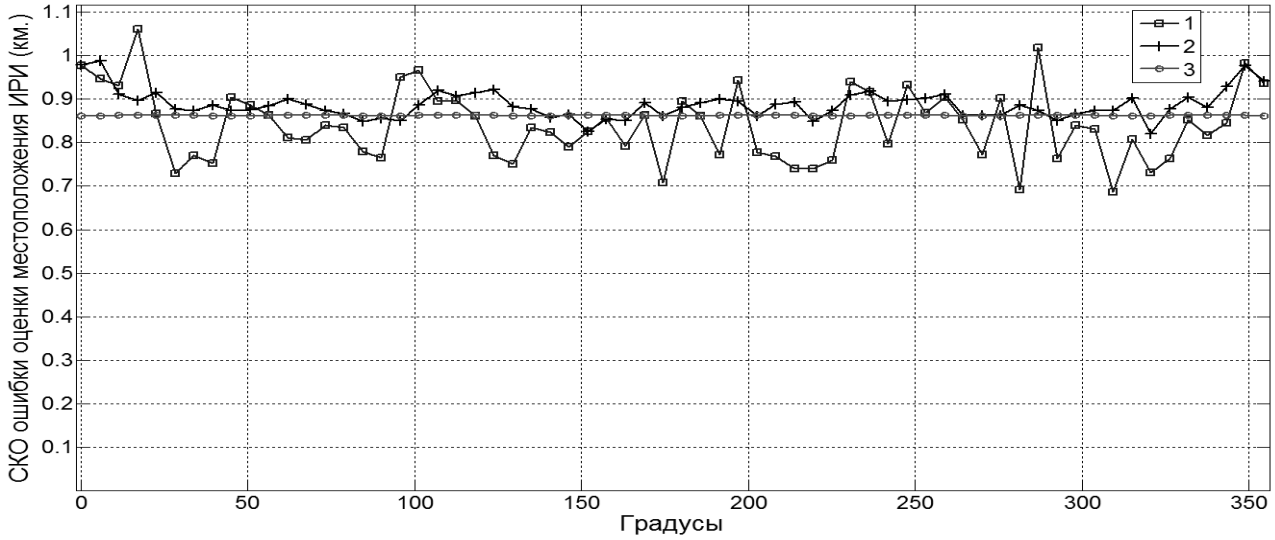


Рис. 2.

Как следует из результатов моделирования для рассмотренного алгоритма СКО погрешности оценки местоположения ИРИ достигает НГРК, Таким образом, он обладает точностными характеристиками, близкими к потенциально достижимым.

Литература

1. Бузуверов Г.В. Алгоритмы пассивной локации в распределенной сети датчиков по разностно-дальномерному методу / Г.В.Бузуверов, О.И. Герасимов. — М. : Информационно-измерительные и управляющие системы №5, 2008. — 12 с.
2. Greg Welch, Gary Bishop. “An Introduction to the Kalman Filter”, Department of Computer Science University of North Carolina at Chapel Hill, July 24, 2006. Available from https://www.cs.unc.edu/~welch/media/pdf/kalman_intro.pdf
3. Симаков В.А. Построение адаптивных систем пассивной радиолокации на принципах разностно-дальномерной координатометрии / В.А. Симаков // Научные ведомости Белгородский государственный университет . — 2005. — №2. — С. 221.

УДК 528.852

МОДЕЛЬ РОЗПОДІЛУ РЕСУРСІВ СЕНСОРНОЇ МЕРЕЖІ НА ОСНОВІ МОДИФІКОВАНОГО ГЕНЕТИЧНОГО АЛГОРИТМУ

Зайцев О.В.
Воєнно-дипломатична академія ім. Євгенія Березняка, м. Київ
E-mail: a_v_zaitsev@ukr.net

Model of resources distribution of sensor network on a basis of the modified genetic algorithm

The mathematical model for maintenance of optimum distribution of information and computing resources among nodes of a sensor network is proposed. The problem of discrete optimisation is formulated. Updating of genetic algorithm which provides special coding for the decision of problems is offered.

Одним з основних напрямів раціонального використання наявних ресурсів сенсорної мережі (з можливістю зберігання результатів спостережень в електронній пам'яті вузла) є територіально розподілене опрацювання даних за єдиним задумом, що пов'язано з необхідністю перерозподілу повноважень серед вузлів з подальшою інтеграцією результатів роботи. Для вдосконалення технології опрацювання інформації передбачається у першу чергу розв'язання проблеми доступу користувачів до ресурсів та реакції системи на запити користувачів за мінімально допустимий час, що великою мірою визначається організацією розподілу інформаційних та обчислювальних ресурсів у локальних і глобальних сенсорних мережах.

Теоретичною та методологічною основою дослідження стали праці в галузі розподілених баз даних та розподілених обчислень таких вітчизняних та зарубіжних вчених, як Г. Цегелик, Н. Куссуль, Я. Фостер, К. Кессельман та ін. [1-5]. Проте актуальними залишаються питання розроблення математичної моделі оптимального розподілу інформаційних та обчислювальних ресурсів серед вузлів сенсорної мережі.

Кількість часу, необхідного для обслуговування запитів на пошук і корегування, залежить від розподілу інформації серед вузлів мережі. Чим менший обсяг даних, що пересилається по каналах зв'язку за одиницю часу, тим більша швидкість опрацювання запитів. У ході роботи системи для кожного блоку даних (наприклад, файлу) виконується певна кількість запитів на пошук і корегування. Очевидно, що оптимальна кількість копій кожного файлу більша за один, але менша кількості вузлів мережі. Розроблена математична модель для визначення оптимальної кількості копій блоків даних (файлів) та їх розподілу серед вузлів комп'ютерних мереж має такий вигляд:

$$L = \sum_{i=1}^{m} \sum_{j=1}^{n} t_{ij} x_{ij} \to \min \quad , \qquad (1)$$

де n – кількість вузлів мережі; m – кількість різних задач, які потрібно розв'язати, t_{ij} – час виконання задачі Z_i на вузлі K_j, x_{ij} – величини, значення яких визначається.

Для пошуку оптимальних або близьких до оптимальних розподілів задач між вузлами комп'ютерної мережі запропоновано модифікований генетичний алгоритм. У запропонованій модифікації генетичного алгоритму розподіл ресурсів зображується у вигляді двійкової послідовності (кодування), завдяки цьому скорочується довжина розподілу і враховуються умови цього розподілу. Блок-схему модифікованого генетичного алгоритму наведено на рис. 1.

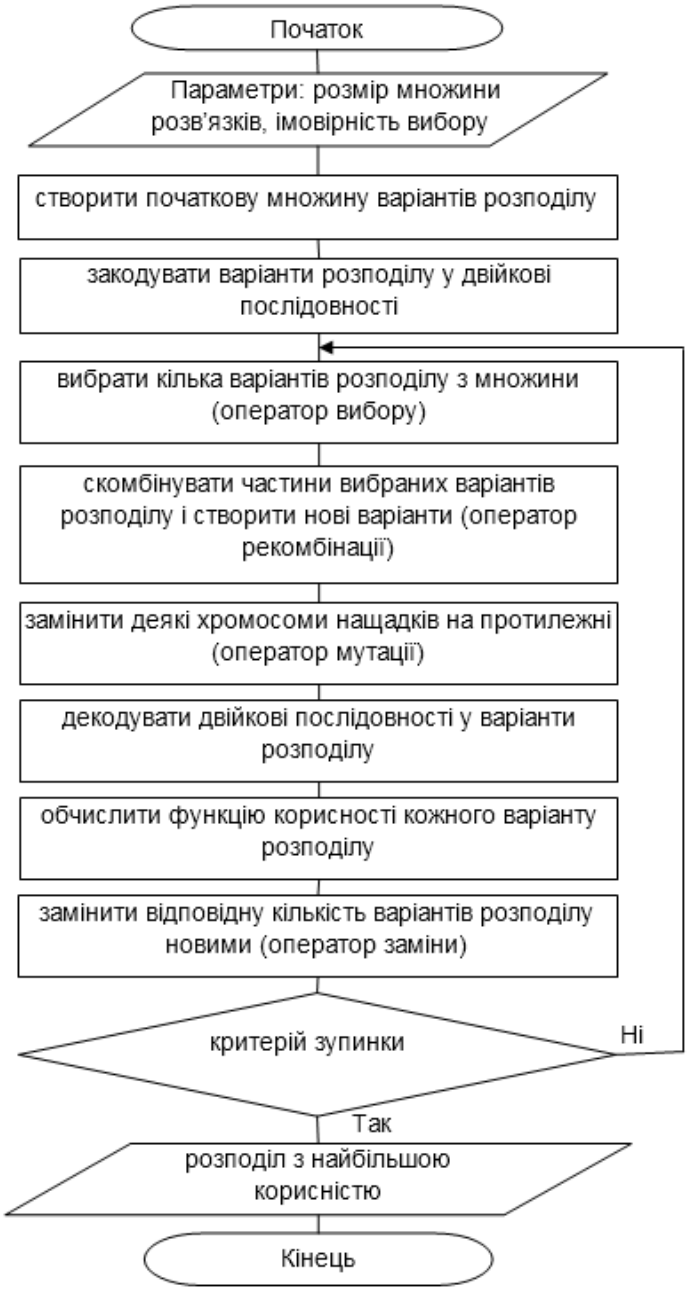


Рис. 1. Блок-схема модифікованого генетичного алгоритму.

Розподіл ресурсів, за визначенням, є двійковим, який, крім мінімізації цільової функції, має задовольняти додатковим умовам (на кількість копій файлів, на обсяг пам'яті, на кількість задач різного типу, на час використання кожного сенсора). Таким чином, довжина двійкового зображення, яке є потенційним розв'язком задачі оптимізації, зменшиться, що дає можливість суттєво скоротити час роботи генетичного алгоритму.

Щоб урахувати умови на обсяг пам'яті, відведеної для зберігання файлів у кожному вузлі, використано методику штрафних функцій, тобто функцію корисності в генетичному алгоритмі задано в такому вигляді:

$$f(X) = L(X) + \sum_{j=1}^{n} A_j \max\left\{0, \left| \sum_{i=1}^{m} L_{ij} x_{ij} - b_j \right| \right\}, \quad (2)$$

де A_j – коефіцієнти масштабування.

Критерієм зупинки генетичного алгоритму зазвичай вибирають максимальну кількість ітерацій. Однак експерименти свідчать, що критерієм зупинки для задачі оптимізації розподілу ресурсів серед вузлів комп'ютерних мереж доцільно вибирати такий:

$$\left| \frac{f_{\max}(P(t))}{f_{avg}(P(t))} - \frac{f_{\max}(P(t-1))}{f_{avg}(P(t-1))} \right| \le \varepsilon, \quad (3)$$

де $f_{\max}$ – максимальне значення функції корисності, f_{avg} – середнє значення функції корисності для всієї множини розподілів ресурсів.

Література

1. Тичковський Р. О. Математичне моделювання оптимального використання потужностей ЕОМ в обчислювальних мережах / Р. О. Тичковський, Г. Г. Цегелик // Тези доп. Всеукр. наук. конф. "Актуальні проблеми аналізу та моделювання складних систем". – Черкаси, 2007. – С. 39.
2. Куссуль Н. Grid-системы для задач исследования Земли. Архитектура, модели и технологии / Н. Куссуль, А. Шелестов. – К.: Наукова думка, 2008. – 452 с.
3. Timothy G. Armstrong Conference Compiler techniques for massively scalable implicit task parallelism: Conference High Performance Computing, Networking, Storage and Analysis, SC14 2014/11/16: International Conference [Електронний ресурс] / Timothy G. Armstrong, Justin M. Wozniak, Michael Wilde, Ian T. Foster // IEEE. – 2014. – P. 299-310. – Режим доступу: http://people.cs.uchicago.edu/~tga/pubs/stc-sub.pdf.
4. Robert E. Schuler An Asset Management Approach to Continuous Integration of Heterogeneous Biomedical Data: Data Integration in the Life Sciences [Електронний ресурс] / Robert E. Schuler, Carl Kesselman, Karl Czajkowski // Springer International Publishing. – 2014. – P. 1-15. – Режим доступу: http://www.hpcc.unical.it/ hpc2014/pdfs/kesselman.pdf.
5. Robert Schuler A flexible, open, decentralized system for digital pathology networks: Studies in health technology and informatics [Електронний ресурс] / Robert Schuler, David E. Smith, Gowri Kumaraguruparan, Ann Chervenak, Anne D. Lewis, Dallas M. Hyde, Carl Kesselman // NIH Public Access. – 2012. – P. 29 (Том 175). – Режим доступу: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3966426/.

УДК 621.396.946

СПОСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В МОБІЛЬНИХ МЕРЕЖАХ

Зубик С. О.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: zubyk.sergey@gmail.com

Way to improve security of mobile networks

Examining types of attacks and way to protect mobile networks, increasing the efficiency of information security through using cryptography algorithms.

This paper gives general information about the standards of mobile communication, described attacks on mobile networks, discussed ways to protect mobile networks and both the GSM and UMTS, the program implemented block cipher KASUMI.

KASUMI – блочний шифр, що використовується в мережах стільникового зв’язку 3GPP, найбільш широке визнання отримав при використанні в мобільних мережах стандарту UMTS, але зараз активно впроваджується в стільниковій мережі GSM, де позначається A5/3. KASUMI був розроблений групою SAGE (Security Algorithms Group of Experts), яка є частиною Європейського Інституту по Стандартизації в області Телекомунікацій (ETSI). За основу був узятий існуючий алгоритм MISTY1 і оптимізований для використання в стільниковому зв'язку.KASUMI використовує 64-бітний розмір блоку і 128-бітний ключ у 8-раундовій схемі Фейстеля. У кожному раунді використовується 128-бітний раундовий ключ, що складається з восьми 16-бітових підключів, отриманих з вихідного ключа фіксованою процедурою генерації підключів.

Алгоритм KASUMIє алгоритмом Фейстеля з різними парними і непарними раундами. У непарних раундах, в порівнянні з парними раундами виконується додатково операція FL, яка також виконується і по завершенні останнього раунду. Кількість раундів дорівнює восьми. На рисунку 1 представлена послідовність операцій, виконуваних при шифруванні даних за алгоритмом KASUMI.

Таким чином, при виконанні операції FL32-бітне вхідне значення розбивається на два блоки по 16 біт, над якими виконуються операція додавання за модулем 2 і побітові логічні операції, причому в логічних операціях беруть участь певні фрагменти розширеного ключа шифрування для операції K_{L1} і K_{L2}.

Більш складною є операція FO. В даній операції 32-бітове вхідне значення також ділиться на два 16-бітових фрагменти, один з яких обробляється операцією додавання за модулем 2 з визначеним фрагментом

ключа для операції FO (K_{Ox}) і операцією FI, після чого значення даних в цих блоках додаються за модулем 2 і міняються місцями.

На відміну від операцій FL і FO, операція FI обробляє 16-бітові блоки вхідних даних.

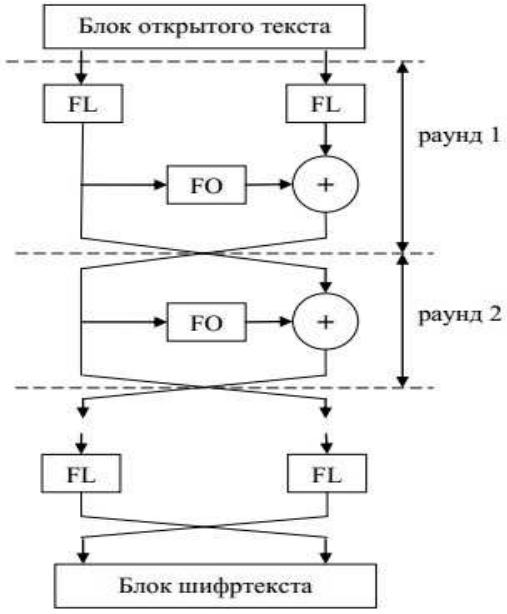


Рис. 1 Послідовність шифрування даних за алгоритмом KASUMI.

Це 3-раундова мережа Фейстеля, яка оброблює 7-бітний і 9-бітний блоки, над якими виконуються наступні операції:

- Табличні заміни S7 і S9 над 7 - і 9-бітовим блоком відповідно;

- Додавання блоків між собою за модулем 2, причому в першому і третьому раундах 7-бітний блок доповнюється нулями, і результатом додавання є 9-бітний блок, а в другому раунді при додаванні відкидаються два лівих біта 9-бітного блоку і результатом додавання є 7-бітний блок;

- Додавання за модулем 2 відповідних блоків з 7- і 9-бітовими фрагментами розширеного ключа шифрування K_{L1} і K_{L2}, що виконується у другому раунді;

Кожен раунд KASUMI отримує ключі із загального ключа K наступним чином:

- 128-бітний ключ K поділяється на 8 ключів: $K = K_1 || K_2 || K_3 || \dots || K_8$;

- Обчислюється другий масив $K_{j'} = K_j \oplus C_j$, де C_j визначається матрицею, яка наведена в таблиці 1.

Таблиця 1. Матриця значень C_j для розрахунку K_j,

C_1	0x0123
C_2	0x4567
C_3	0x89AB
C_4	0xCDEF
C_5	0xFEDC
C_6	0xBA98
C_7	0x7654
C_8	0x3210

- Ключі для кожного раунд обчислюються, як показано в таблиці 4.2

Таблиця 2. Розрахунок ключів для кожного раунду.

Ключ	1	2	3	4	5	6	7	8
$KL_{i,1}$	K1<<<1	K2<<<1	K3<<<1	K4<<<1	K5<<<1	K6<<<1	K7<<<1	K8<<<1
$KL_{i,2}$	K3'	K4'	K5'	K6'	K7'	K8'	K1'	K2'
$KO_{i,1}$	K2<<<5	K3<<<5	K4<<<5	K5<<<5	K6<<<5	K7<<<5	K8<<<5	K1<<<5
$KO_{i,2}$	K6<<<8	K7<<<8	K8<<<8	K1<<<8	K2<<<8	K3<<<8	K4<<<8	K5<<<8
$KO_{i,3}$	K7<<<13	K8<<<13	K1<<<13	K2<<<13	K3<<<13	K4<<<13	K5<<<13	K6<<<13
$KI_{i,1}$	K5'	K6'	K7'	K8'	K1'	K2'	K3'	K4'
$KI_{i,2}$	K4'	K5'	K6'	K7'	K8'	K1'	K2'	K3'
$KI_{i,3}$	K8'	K1'	K2'	K3'	K4'	K5'	K6'	K7'

Шифр KASUMI реалізується функцією безпеки f_8в стандартах UMTS та CDMA, причому він функціонує в режимі зворотного зв'язку, де функція f_8 використовується для генерування блоків ключового потоку, які побітово додаються до блоків відкритого тексту за модулем 2.

У 2009 році було опубліковано атаку на KASUMI «методом бумерангу», який зламує шифр швидше, ніж повний перебір. Складність атаки дорівнює 2^{76}, що порівняно з алгоритмомA5/1, для якого складність атаки складає 2^{40}, більше на 10-ки порядків. Отже шифр KASUMI є найбільш криптостійким і є оптимальним вибором для шифрування інформації в мобільних мережах.

Література

1. Ветров Ю.В. Криптографические методы защиты информации в телекоммуникационных системах: учеб. пособие / Ю.В. Ветров, С.Б. Макаров. - СПб.: Издательство Политехника ун-та, 2011. - 174 с.
2. *Куприянов А.И., Сахаров А.В., Швецов В.А.* Основы защиты информации: учебное пособие для студентов высших учебных заведений. – М.: Издательский центр «Академия», 2006. – 256 с.
3. *Чекалин А.А., ЗаряевА.В.* Защита информации в системах мобильной связи: Учебное пособие для вузов. - М.: Горячая линия – Телеком, 2005. - 171с.
4. *Ярочкин В.И.* Безопасность информационных систем (Безопасность предпринимательства). – М.: Ось-89, 1996. – 318 с.

УДК 621.396

ГІБРИДНИЙ МЕТОД ВИЗНАЧЕННЯ КООРДИНАТ ВУЗЛІВ БЕЗПРОВОДОВОЇ СЕНСОРНОЇ МЕРЕЖІ

Кашуба С.В., Лисенко О.І.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: kashubasv@gmail.com

Hybrid Localization Method for Wireless Sensor Network Nodes

Wireless sensor network applications require node localization. In some scenarios, explicit node positioning (e.g. GPS) is not possible. In a case of sparse nodes placement or nodes mobility distance oriented localization methods lose robustness. To cope with increased equipment complexity of angle oriented localization methods we propose hybrid approach. Distance and angle measurements are provided by nodes of different type and used after exchange for each node positioning.

Безпроводові сенсорні мережі (БСМ) складаються з великої кількості автономних вузлів, що призначені для оперативного збору та передачі даних про фізичне середовище. Інформація про координати окремих вузлів є дуже важливою для БСМ оскільки застосування таких мереж часто пов’язано з моніторингом великих ділянок місцевості або відслідковуванням рухомих об’єктів. Крім того, деякі енергоефективні протоколи маршрутизації базуються на використанні інформації про просторове розміщення елементів мережі [1]. Безпосереднє визначення координат кожного окремого вузла мережі (наприклад, з допомогою вбудованого GPS приймача) може бути проблематичним через конструктивні обмеження вузлів або неможливість надійного прийому від супутників позиціонування.

Більшість алгоритмів позиціонування вузлів БСМ використовує абсолютні координати невеликої кількості точок (анкери) та вимірювання відносного розташування між рештою вузлів (внутрішнє позиціонування). Абсолютні позиції анкерних вузлів можуть бути визначені за допомогою глобальної системи позиціонування або при розгортанні мережі, якщо такі вузли є стаціонарними [2].

Існує декілька базових математичних методів визначення взаємного положення вузлів на площині з використанням [3]:

- напрямку (азимут) відносно двох точок з відомими координатами;
- відстані від трьох точок з відомими координатами;
- відстані та напрямку відносно однієї точки.

Відстань між вузлами БСМ може бути визначена через затримку прибуття сигналу (Time of Arrival), різницю часу прибуття (Time Difference of Arrival), потужність прийнятого сигналу (Received Signal Strength). Напрямок розташування відносно іншого вузла в БСМ може бути визначено за допомогою направлених антенних систем. Такі системи можна реалізувати завдяки компактним (декілька елементів) фазованим антенним решіткам [4]. Вимушене ускладнення вузла та збільшення його габаритів є значним

обмеженням для алгоритмів позиціонування, що використовують інформацію про напрямок розміщення сусіднього сенсора.

Серед реалізацій визначення взаємного розміщення вузлів БСМ слід виділити метод відстані до трьох точок з використанням потужності прийнятого сигналу. Метод гарантує певну точність визначення координат та є простим в реалізації: функції виміру рівня прийнятого сигналу вже вбудовані у сучасні радіомодулі, а точність перевершує методи на основі топології мережі. Проте, модель розповсюдження радіосигналу може давати неточні оцінки відстані в нестійких реальних умовах поширення сигналу. Інше обмеження - необхідність досить щільного розташування вузлів (принаймні 3 сенсори в радіусі передачі).

Визначення координат на основі напрямку розташування одних вузлів відносно інших вимагає менше опорних точок, але пов’язано з технічним ускладненням сенсорів. У такій ситуації постає питання можливості використання гібридного підходу.

У основі запропонованого рішення лежить одночасне використання інформації про відстань та напрям розміщення сусідніх вузлів. Проте, для зменшення вартості мережі функції вимірювання відстані та напрямку розділені між вузлами різних типів. Таким чином мережа складається з сенсорів, що можуть визначити відстань до сусідніх вузлів у зоні радіозв’язку, та з вузлів, що володіють інформацією про просторовий напрямок розміщення сусідів.

На рис.1 приведено ілюстрацію фрагменту БСМ, та послідовність взаємодії вузлів для визначення їх координат. Вузли S1 та S3 можуть визначати відстань до сусідів, а вузол S2 азимут їх розташування відносно своєї позиції. Вузли розміщені так, що відстань між S1 та S3 перевищує радіус радіозв’язку та визначення відстані. Приймемо, що вузол S1 є анкерним і володіє інформацією про власні точні координати (приймач GPS).

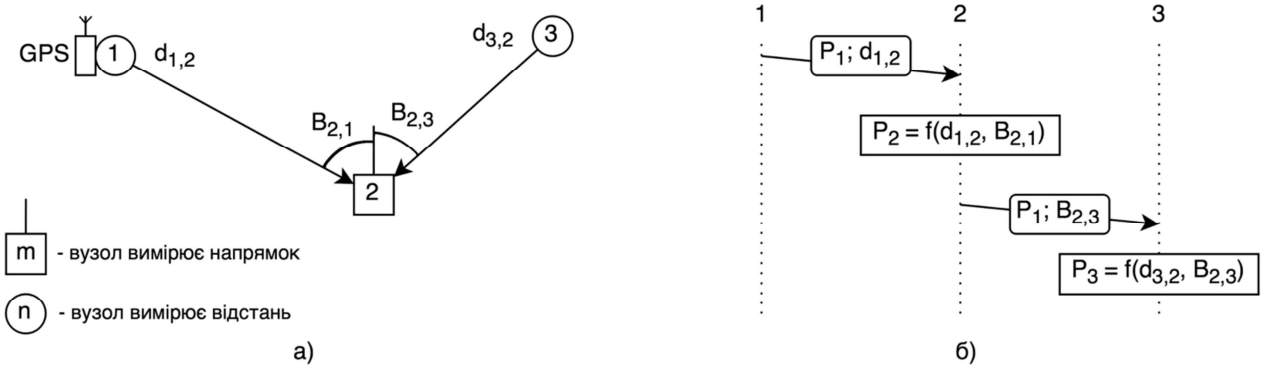


Рис.1 Фрагмент мережі з вузлами різного призначення -а);
послідовність поширення інформації про координати вузлів – б).

На першому етапі відбувається вимірювання інформації про розташування сусідніх вузлів. Таким чином S1 визначає відстань до S2, S2 - азимути розміщення вузлів S1 та S3, а S3 - відстань до S2. Далі відбувається обмін виміряною інформацією між вузлами та поширення вже відомих координат вузлів. S2 отримує координати опорного S1 та відстань до нього,

чого разом з власними вимірюваннями є достатньо для визначення абсолютних координат. Аналогічно, S2 передає напрямок свого розміщення та визначені координати до S3.

У залежності від типу сусідніх вузлів та їх кількості алгоритм поширення координат від опорних вузлів може відрізнятися для певних фрагментів мережі. Наприклад, у випадку щільного розміщення вузлів з вимірюванням відстані, мережа може використовувати метод відстані до трьох точок.

Хоча принцип реалізації описаного методу є досить простим, його практичне використання потребує ряду досліджень. По-перше, ефективність методу залежить від співвідношення кількості вузлів різних типів. Вірогідно, що для випадків випадкового та систематичного розміщення вузлів кількість вузлів може визначатися різними способами. По-друге, фізичні характеристики вузлів різного типу можуть відрізнятися. На приклад, вузли вимірювання напрямку мають направлену антенну систему, що дозволяє при тій же потужності збільшити радіус передачі порівняно з вузлами вимірювання відстані.

Запропонований гібридний метод визначення координат вузлів БСМ може використовуватися в умовах низької щільності розміщення сенсорів, коли в радіусі радіоканалу знаходиться лише один чи декілька сусідніх вузлів, або в умовах рухомих сенсорів (мобільні БСМ), коли важко гарантувати досяжність необхідної кількості опорних вузлів для методів локалізації по відстані.

Література

1. Hu L. Localization for mobile sensor networks / L. Hu, D. Evans // In Proceedings of the 10th annual international conference on Mobile computing and networking, pp. 45–57. ACM, 2004.
2. Mao G. Wireless sensor network localization techniques / G. Mao, B. Fidan, B. Anderson // Computer Networks, 51(10), pp. 2529 – 2553, 2007.
3. Chaczko Z. Methods of sensors localization in wireless sensor networks / Z. Chaczko, R. Klempous, J. Nikodem, M. Nikodem // In Engineering of Computer-Based Systems, 2007. ECBS’07. 14th Annual IEEE International Conference and Workshops, pp. 145–152. IEEE, 2007.
4. Kulakowski P. Angle-of-arrival localization based on antenna arrays for wireless sensor networks / P. Kulakowski, J. Vales-Alonso, E. Egea-Lopez, W. Ludwin, J. Garcia-Haro // Computers & Electrical Engineering, 36(6), pp. 1181–1186, 2010.

УДК 519.711.3

МЕТОД АДАПТАЦІЇ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ ПОБУДОВАНИХ НА РАДІОГІДРОАКУСТИЧНИХ БУЯХ ДО УМОВ ФУНКЦІОНУВАННЯ

Кутельова О.С., Великий О.О., Петрова В.М.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: olga.kuteleva@gmail.com, a.a.velikiy@gmail.com

Method of adaptation of wireless sensor networks built on the radio sonar sonobuoys for condition functioning

Experimentally proven resource cost reduction in the design, deployment and operation of wireless sensor networks built on radio sonar sonobuoys using algorithmic and software implementation of a rational calculation of network topology with the possibility of its practical play. This system is used to monitor water waters (pollution, level radioactive waste, etc.) as well as in the military field to determine the deployment of ships and submarines of the enemy.

Актуальними залишаються проблеми пов’язані з пошуком об’єктів на водних акваторіях (кораблів, підводних човнів, тощо), нафтових продуктів, тощо. Сенсорна мережа побудована на радіогідроакустичних буях – макротехнологія подвійного призначення, може бути використана як у цивільних (виявлення джерел нафтових забруднень), так і у військових (для захисту водних кордонів) цілях. Застосовуються з метою виявлення підводних човнів та інших підводних об'єктів, зв'язку з підводними човнами, а також у наукових цілях. Гідроакустичний буй (також радіогідроакустичний буй, РГБ) - вільно плаваючий або встановлений на якорі буй, призначений для випромінювання та / або прийому та ретрансляції по радіоканалу гідроакустичних сигналів. Застосовуються з метою виявлення підводних човнів та інших підводних об'єктів, зв'язку з підводними човнами, а також у наукових цілях (знаходження місця розливу нафтопродуктів, тощо). Як правило, скидаються з літака, вертольоту або надводного корабля. Після потрапляння у воду протягом певного часу автоматично приводяться в робоче положення. При цьому з донної частини поплавця на кабелі опускається на певну глибину приймач і / або передавач гідроакустичних коливань. Ухвалений гідроакустичний сигнал по УКХ-радіоканалу ретранслюється на літак або корабель-носій у вигляді частотно-модульованого сигналу [1].

Сучасні РГБ забезпечують гнучкість пошуку підводних човнів (об’єктів) в різних тактичних ситуаціях завдяки можливості зміни глибини занурення гідрофонів, а також вибору схеми постановки бар'єрів або полів.

Основною проблемою БСМ залишається визначення оптимальної кількості сенсорів, ефективно обслуговувану площу, потрібний запас енергоносіїв (акумуляторних батарей), оптимальна топологія БСМ і т.д. [2].

Для підвищення ефективності БСМ запропоновано використати експертно-моделюючу систему (ЕМС). Існує множина проектів {Т1, …, Tk}. Для прийняття рішення про впровадження проекту БСМ побудованої на радіогідроакустичних буях (РГБ) залучають групу експертів, які виконують

експертизу із застосуванням системної методології передбачення. Це дозволило: розробити для БСМ побудованої на РГБ ієрархічну систему критеріїв оцінки ефективності їх функціонування, удосконалити метод вибору найкращого варіанту в умовах невизначеності, розробити експертно-моделюючий комплекс імітаційних моделей для перевірки прийнятих рішень [3].

Метод отримання експертно-моделюючої системи. На рис.1 зображений метод експертної оцінки показників якості БСМ побудованих на РГБ.

Побудова системи критеріїв оцінки ефективності БСМ побудованої на РГБ відображає розрахунки експертами ефективності БСМ побудованої на РГБ, а саме: визначення оптимальної кількості сенсорів, оптимальну топологію мережі, обслуговувану площу, потрібний запас енергоносіїв і т.д., при зібранні та аналізуванні інформації про потрібну БСМ побудованої на РГБ. Також будуються сценарії розвитку можливих ситуацій при експлуатації БСМ побудованої на РГБ, розраховуються обсяги та масштаби.

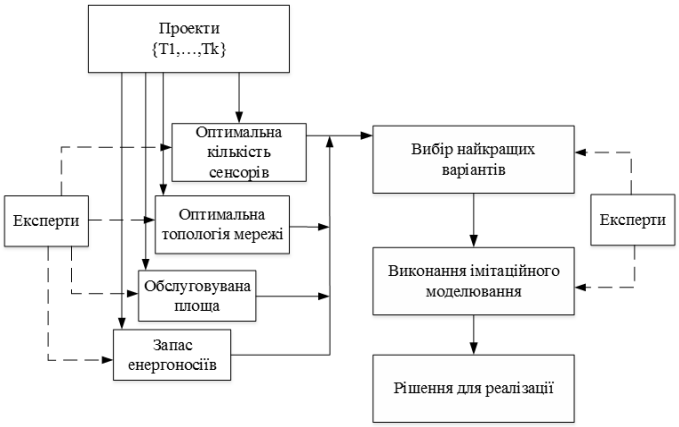


Рис.1 Удосконалена модель експертизи проектів БСМ побудованої на РГБ

Після зібраних варіантів, аналізу всіх критеріїв, робиться вибір найкращих варіантів із запропонованих. Заповнюється матриця, яка містить сценарії {C1,…,Cn}, та {T1,…,Tm} – проекти ТКС зони лиха. Кожен проект містить всі сценарії, за який експерти виставляють умовні оцінки їх доцільності і ефективності. Вибір найкращого варіанту проводиться за допомогою методів теорії ігор (критерієм Вальда, критерієм Севіджа, критерієм Гурвиця).

Для практичного застосування вибраних варіантів, виконується імітаційна модель, а також розрахунки ефективності тієї чи іншої системи (Рис.2).

Результати моделювання. Всі розрахунки накладаються на топографічну карту місцевості, з якого можна зробити висновок щодо досконалості мережі, які компоненти потрібно добавити, чи замінити. Вибирається певний вид РГБ, який краще підходить для виконання конкретного завдання, чи то моніторинг водних акваторій на рахунок допустимих рівнів радіації чи викидів шкідливих речовин у водні ресурси, чи моніторинг водних акваторій на предмет перебування/пересування військових об’єктів.

Рис.2 Виконання імітаційного моделювання БСМ побудованої на РГБ.

Після цього можна ще раз розрахувати БСМ, і отримати результат задовольняючої мережі. За результатами робиться висновок, яка із запропонованих систем краще підходить для даної БСМ побудованої на РГБ, і приймається рішення на реалізацію даного методу (див. рис. 3) [4].

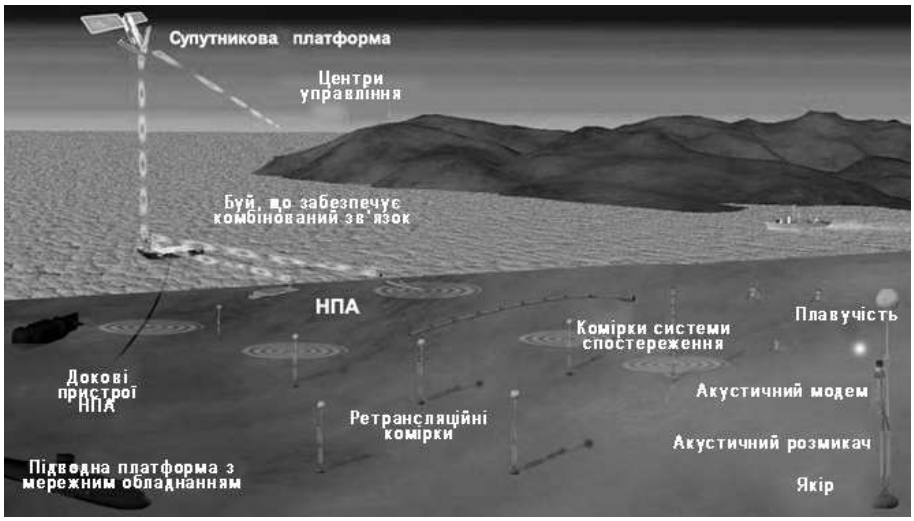


Рис.3 БСМ побудована на РГБ розрахована за допомогою ЕМС.

Таким чином, за допомогою ЕМС підвищується ефективність проектування і використання БСМ побудованих на РГБ (об'єктивно визначаються недоліки і система допрацьовується). Оптимальні значення кожного з параметрів системи та умов замовника призводить БСМ побудованої на РГБ до максимально ефективного використання.

Література

1. Лаверов Н. П., Рослов Ю. В., Лобковский Л. И. и др. «Перспективы донной сейсморазведки в Российской Федерации» // Арктика: экология и экономика. - 2011. - № 4.
2. Великий А.А., Лисенко О.І. «Метод експертної оцінки показників телекомунікаційних систем зони лиха в умовах деструктивних впливів» // Восьма міжнародна науково-технічна конференція «Проблеми Телекомунікацій. – 2014.
3. Сложные технические и эргадические системы: метод использования / А. Н. Воронин, Ю. К. Зиатдинов, А. В. Харченко, В. В. Осташевский. – Х. : Факт, 1997. – 240 с.
4. Y. Noh, U. Lee, Member, P. Wang,: VAPR: Void Aware Pressure Routing for Underwater Sensor Networks, Proc. IEEE (2014).

УДК 621.391

МЕТОД АДАПТИВНОГО УПРАВЛЕНИЯ МАРШРУТИЗАЦИЕЙ В УСЛОВИЯХ НЕСТАБИЛЬНОСТИ СВЯЗЕЙ МЕЖДУ УЗЛАМИ БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТИ

Лысенко А.И., Новиков В.И.
Институт телекоммуникационных систем НТУУ «КПИ»
E-mail: novikov1967@ukr.net

Routing adaptive control method in the case of unstable relations between wireless sensor network nodes

Proposed a routing control method in wireless sensor networks with dynamic topology in the case of unstable relations between their nodes. The method based on dynamic choosing a target route control function with considering routing types and the unstable connection between wireless sensor network nodes.

Одной из основных задач оперативного управления беспроводными сенсорными сетями (БСС) является маршрутизация информационных потоков. Анализу и синтезу методов маршрутизации в БСС посвящено большое количество работ [1–2]. Проведенный анализ существующих методов маршрутизации показал, что каждый метод эффективен при определенной ситуации в сети (динамика изменения топологии, интенсивность входящего трафика, размерность и т. д.). Кроме того, существующие методы маршрутизации ориентированы на работу в условиях стабильности радиоканалов между соседними узлами БСС и не учитывают влияние нестабильности связей между узлами сети, что может оказать негативное влияние на эффективность маршрутизации в целом.

Для достижения эффективного функционирования БСС в условиях нестабильности связей между ее узлами предложено использовать новый адаптивный метод управления маршрутизацией, обеспечивающий оптимизацию показателей эффективности функционирования сети при различных условиях ее работы.

Метод адаптивного управления маршрутизацию предусматривает следующие подходы: функционирование в сети не одного, а множества методов маршрутизации; динамическое формирование метрик выбора маршрута с учетом нестабильности связей между узлами БСС; управление топологией сети как составной частью маршрутизации в БСС; интеллектуализацию процессов принятия решения по маршрутизации.

Раскроем подробнее содержание составляющих компонент метода адаптивного управления маршрутизацией.

Параллельное функционирование множества методов маршрутизации (ММ) и ситуационное управление их применением. Каждый узел сети реализует множество методов маршрутизации $\{MM\} = \{MM_1, MM_2, \ldots, MM_n\}$. В зависимости от конкретной ситуации на сети функционирует один из них – MM_i, который обеспечивает сетевую оптимизацию. Ситуационное

управление маршрутизацией может осуществляться по ряду параметров функционирования сети: типу передаваемой информации, изменению топологии, размерности и площади сети, входящему трафику, плотности размещения узлов и их взаимного расположения и т.п.

Динамическое формирование метрик выбора маршрута с учетом нестабильности связей между узлами беспроводной сенсорной сети. Данный подход предполагает активный поиск необходимого маршрута: маршрутное сообщение несет в себе требования к маршруту в виде параметров (метрик) выбора маршрута и программу его обработки. Большинство предложенных методов маршрутизации использует однопараметрическую маршрутизацию, которая при выборе кратчайшего пути учитывает только один параметр. В условиях нестабильности связей между узлами беспроводной сенсорной сети необходимо дополнительно использовать метрики стоимости соединения, учитывающие потери пакетов в реальных радиоканалах[3].

Маршрутизация с управлением топологией сети. Для повышения эффективности функционирования БСС функции маршрутизации реализуются на двух уровнях: на верхнем – оперативное управление топологией сети U_T (создание потенциальных маршрутов передачи информации); на нижнем – управление построением и поддержанием маршрутов при полученной топологии $U_м$ (реализация конкретного метода маршрутизации из их совокупности). Целью управления топологией является системная ($max\ S,\ min\ t_з,\ max\ T_ж$) или пользовательская оптимизация. Задача управления топологией БСС сводится к задаче ситуационного управления с правилами продукционного типа.

Интеллектуализация процессов принятия решений. Рассмотрим архитектуру сенсорного узла, позволяющую реализовать метод адаптивного управления маршрутизацию. Она содержит следующие основные блоки: базу данных управления; классификатор; планировщик; блок обучения; базу знаний, интерпретатор. Рассмотрим возложенные на них функции (рис. 1.).

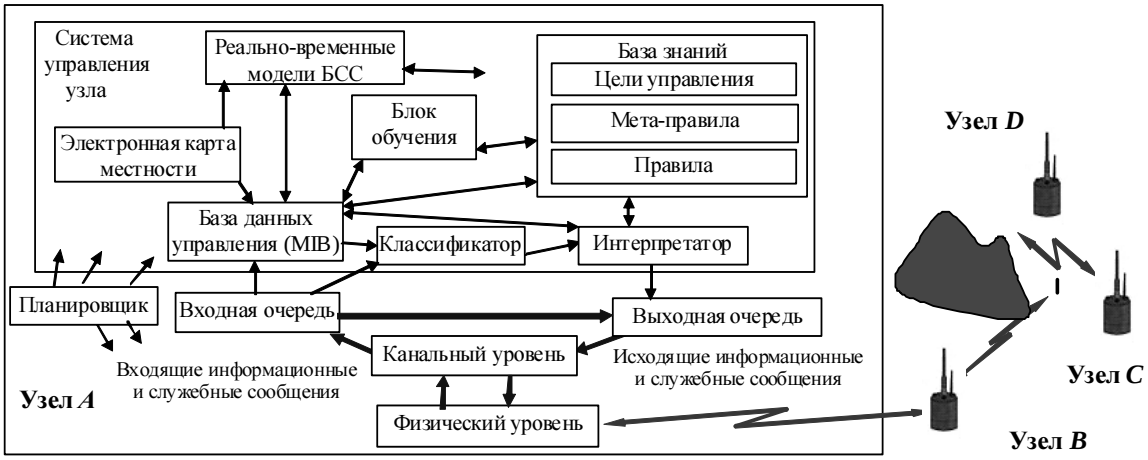


Рис. 1 Архитектура сенсорного узла.

База данных управления MIB (Management Information Base) поддерживает в актуальном состоянии модель узла (сети) и может быть формализована l группами признаков.

Классификатор на основе поступающей на его вход информации осуществляет классификацию принимаемых сообщений, идентификацию текущей ситуации и определяет необходимость управляющего воздействия.

Реально-временные модели предназначены для расчета времени существования маршрута на основании моделей распространения радиоволн, рельефа местности, прогнозируемых параметров трафика и т. д.

База знаний содержит следующую совокупность правил для выработки решений по маршрутизации: определение текущей целевой функции управления, выбор методов и функций маршрутизации, определение формата маршрутной информации (МИ) и др.

Интерпретатор правил выполняет две функции: во-первых, просмотр существующих правил из базы данных и правил из базы знаний и добавление в базу данных новых фактов и, во-вторых, определение порядка просмотра и применения правил. Правила базы знаний работают согласно различным стратегиям. Одни правила обнаруживают перегруженный участок сети и пытаются направить сообщения, минуя его, другие – находят недоиспользованные маршруты и пытаются направить трафик по этим путям, третьи – анализируют топологию сети и пытаются осуществить сетевую оптимизацию. Выбор той или иной цели управления (постановка цели), как и вывод решения, зависят от ситуации и типа передаваемого сообщения на сети.

Таким образом, в дополнение к традиционным функциям маршрутизации (сбор, хранение маршрутной информации, построение маршрута и передача входящего пакета согласно маршрутным таблицам) метод адаптивного управления маршрутизацию позволяет осуществлять сетевую и пользовательскую оптимизацию за счет адаптации к текущей ситуации на сети, типу передаваемой информации и повышения уровня обоснованности принимаемых маршрутных решений.

Литература

1. Міночкін А.І, Романюк В.А., Жук О.В. Перспективи розвитку тактичних сенсорних мереж // Збірник наукових праць № 4. – К.: ВІТІ НТУУ “КПІ”. – 2007. – С. 112 – 119.
2. Бунин С.Г., Войтер А.П., Ильченко М.Е., Романюк В.А. Самоорганизующиеся радиосети со сверхширокополосными сигналами. – К.: НПП «Издательство «Науковадумка» НАН Украины». –2012. - 444 с.
3. Новіков В.І. Метрики вартості з´єднання та прогресу для вирішення завдань маршрутизації в безпроводових сенсорних мережах // Науковий вісник АМУ, Збірник наукових праць, Серія "Техніка", Випуск 2 (8), 2014. - С. 99-112.

УДК 621.39

АНАЛІЗ МЕТОДІВ ТА ПРОТОКОЛІВ УПРАВЛІННЯ В БЕСПРОВОДНИХ СЕНСОРНИХ МЕРЕЖАХ

Остапенко О.О. Романюк В.А. Жук А.В.
Військовий Інститут Телекомунікацій та Інформатизації ДУТ
E-mail : ostapenko86@icloud.com, romval2016@ gmail.com, beatle135@ukr.net

Methods' analysis (protocols) management in wireless sensor networks

Methods' analysis (protocols) management in wireless sensor networks have been considered. The proposals on the synthesis and development management at different levels of the reference model of open systems have been given.

Безпровідні сенсорні мережі (БСМ) або *Wireless Sensor Network* (WSN) – розподілені мережі, що складаються з маленьких сенсорних вузлів, з інтегрованими функціями моніторингу навколишнього середовища, обробки і передачі даних [1].

На даному етапі існує ряд труднощів для побудови безпровідних сенсорних мереж різних напрямків призначення, при цьому вирішити ряд наукових завдань (маршрутизація, управління потужністю, управління топологією, управління енергоресурсом, безпека, забезпечення заданої якості передачі і т. п.) при обмеженнях ресурсу радіотерміналу (місткість пам'яті, продуктивність процесу, місткість батареї).

Канальний рівень. Детальний факторний аналіз, проведений в [2], показав, що: – ефективність методу доступу в сенсорних мережах залежить не тільки від вхідного навантаження, а також від мобільності вузлів, використовуваного методу маршрутизації і поточної топології мережі; – не існує єдиного методу доступу (або комбінації метод доступу/метод маршрутизації), що забезпечують ефективне функціонування мережі за різних умов. Вибір (синтез) необхідного методу доступу не можна розглядати ізольовано від інших рівнів еталонної моделі взаємодії відкритих систем. Він визначатиметься параметрами сенсорної мережі (розмірністю, мобільністю, оснащеністю вузлів, обладнанням позиціювання, спрямованими антенами і ін.), параметрами інформаційного навантаження і вимогами до її передачі, а також ухваленими рішеннями на інших рівнях.

Мережевий рівень (маршрутизація). Аналіз наведений в [3] показав неспроможність існуючих протоколів маршрутизації задовольнити вимогам, які пред'являються до перспективних сенсорних безпровідних мереж. При розробці протоколів маршрутизації для сенсорних мереж необхідно враховувати наступні фактори: – тип навантаження та періодичність (функцію) генерації навантаження; – обмежену кількість адресатів (отримувачів) сенсорної інформації; – обмежену енергоємність батарей вузлів та необхідність підвищення тривалості функціонування сенсорної мережі. Процес управління маршрутизацією повинен бути орієнтований на поточний стан сенсорної мережі

(наявність цілей – джерел інформації, розмірність мережі, потужність сенсорів і т. п.).

Транспортний рівень. Основною проблемою управління навантаженням на транспортному рівні є втрата пакетів. Проте, у відмінності від проводових мереж передачі даних, в яких втрата пакетів може відбуватися, в основному, через локальні перевантаження на окремих вузлах мережі, в безпровідних мережах існує багато причин втрати пакетів, через які стандартний протокол транспортного рівня TCP втрачає свою ефективність. Аналіз приведений в [4] показав що: зараз існує багато робіт з адаптації протоколу TCP для використання в мобільних мережах, проте вони, в основному, враховують тільки окремі особливості безпровідного середовища (C3TCP, TCP-MEDX), або вимагають істотної модернізації мережевого устаткування, яке успішно використовується в даний час (TCP Vegas). Тому для ефективного функціонування протоколів транспортного рівня необхідно розробити механізм, який би давав можливість чітко і точно визначити причину втрати пакетів (внаслідок перевантажень, або помилок в мережі).

Безпека. Проведений аналіз існуючих методів виявлення вторгнень показав, що існуючі методи в основному здатні вирішувати завдання з виявлення вторгнень у провідних або стаціонарних мережах, тому при побудові реальних систем виявлення вторгнень необхідно проводити комбінування методів виявлення вторгнень виходячи з вимог, які будуть визначатися способом управління мережею, місцем та особливостями застосування, типом та розмірністю сенсорної мережі тощо. У ході подальших досліджень буде розроблена функціональна модель СВВ для БСМ та методи виявлення вторгнень із застосуванням технологій інтелектуальних багатоагентних систем та нейронних мереж [5].

Якість обслуговування (QoS, Quality of Servicesы). У Інтернет модель QoS визначена трьома основними рівнями сервісу: сервіс "без гарантії доставки" (Best-effort service), диференційований сервіс – певному класу трафіка віддається перевага при обслуговуванні, гарантований сервіс – повне (абсолютне) резервування мережевих ресурсів для трафіка певного класу. На сьогоднішній день для сенсорних мереж запропоновано ряд QoS-моделей управління [6]: INSIGNIA, FQMM (Flexible QOS Model for MANETs), iMAQ (Integrated MANET QOS), SWAN (Service Differentional in Wireless Ad hoc Networks), 2LQoS (Two-Layer QOS) та ін. Проте вони передбачають управління якістю на певному рівні еталонної моделі взаємодії відкритих систем (ЕМ ВОС) і реалізують прості алгоритми адаптації і резервування ресурсів вузлів (каналів) до різного типу трафіка.

Фізичний рівень. Необхідна адаптація до швидких змін параметрів радіоканалу. Сенсорні мережі повинні відповідати наступним характеристикам: мобільність (підтримання частоти і адаптації до загасання каналу на фізичному рівні); адаптація каналу з використанням кодів, що корегують; зміна потужності передачі (з метою мінімізації перешкод, мінімізації затримки, максимізації пропускної спроможності та ін.).

Енергозбереження. Аналіз енергозберігаючих методів показав що, управління витратами енергоресурсу вузлів повинне здійснюватися за функціями управління на різних рівнях еталонної моделі взаємодії відкритих систем. Проведені дослідження показали, що застосування розглянутих методів дозволяє в середньому збільшити тривалість функціонування мережі в 1, 5…2 рази і зменшити середню потужність передачі на одну ділянку ретрансляції на 10%. Синтез оптимального методу управління витратами енергоресурсу вузлів (або їх сукупності) визначатиметься характеристиками конкретної мережі і ухваленими рішеннями з реалізації інших функцій управління мережею.

Висновки: Проведений аналіз показав неспроможність існуючих методів (протоколів) управління на різних рівнях еталонної моделі взаємодії відкритих систем (Open system interconnection) задовольнити всім вимогам, які пред'являються до сенсорних мереж. Пропонується на *канальному рівні* застосування конкретного методу доступу визначати поточною метою управління мережею, її станом і ухваленими рішеннями на інших рівнях еталонної моделі. Для ухвалення рішення по використанню конкретного методу (в умовах відсутності повної інформації про стан мережі) доцільно використовувати методи нечіткого ситуативного управління. *На мережевому рівні* процес управління повинен бути орієнтований на поточний стан сенсорної мережі (наявність цілей - джерел інформації, розмірність мережі, потужність сенсорів і т. п.). На *транспортному рівні* необхідно розробити метод (протокол), який би давав можливість чітко і точно визначити причину втрати пакетів (внаслідок перевантажень, або помилок в мережі). *На фізичному рівні* необхідна адаптація до швидких змін параметрів радіоканалу: мобільність (підтримання частоти і адаптації до загасання каналу на фізичному рівні); адаптація каналу з використанням кодів, що корегують; зміна потужності передачі (з метою мінімізації перешкод, мінімізації затримки, максимізації пропускної спроможності та ін.). Для *управління безпекою* пропонується розробити гібридний метод із застосуванням технологій інтелектуальних багатоагентних систем та нейронних мереж.

Литература

1. *Міночкін А.І. , Романюк В.А., Жук О.В.* Перспективи розвитку тактичних сенсорних мереж. // Збірник наукових праць ВІТІ НТУУ "КПІ"– 2007. – № 4. С. 16 – 22.
2. *Barlett C., Drozda m., Marathe A.* Analysis Interaction Between Networks Protocols, Topology and Traffic in Wireless Radio Networks // In Proceedings WCNC'03, 2003.
3. *Жук О.В., Сова О. Я., Романюк В.А*. Аналіз протоколів маршрутизації які використовуються при передачі інформації в бездротових сенсорних мережах. // Збірник наукових праць ВІТІ НТУУ "КПІ"– 2008. – № 1. С. 51 – 63.
4. *Міночкін А.І. , Романюк В.А., Сова О.Я*. Аналіз методів управління навантаженням в мобільних радіомережах на транспортному рівні моделі OSI. Збірник наукових праць ВІТІ НТУУ "КПІ" – № 3. – 2006.
5. *Сальник С. В., Сова О. Я., Міночкін Д.А*. Аналіз методів виявлення вторгнень у мобільній радіомережі класу MANET // Сучасні інформаційні технології у сфері безпеки та оборони № 1. – (22)/ 2015.
6. *M. Perillo, W. Heinzelman*. Sensor management policies to provide application QoS, Ad Hoc Networks (Elsevier) 1 (2–3) (2003) 235–246.

УДК 621.3

ВИКОРИСТАННЯ ПЛАТФОРМИ NODE.JS ДЛЯ РОЗРОБКИ СУЧАСНИХ ВЕБ-СЕРВІСІВ

Остапенко С.О., Прищепа Т.О.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: serg.ostapenko94@gmail.com

Usage of Node.js platform for web-application development

Node.js - platform for developing high-load server-side web applications. Synchronous and asynchronous input - output model. Advantages of using technology for developing multi-user applications. Common mistakes in the use of Node.js. Huge growth in popularity of technology.

Завдяки зростаючій популярності, мова JavaScript в наш час активно розвивається, а сучасні бізнес-процеси, зазнали значних змін в порівнянні з недавнім минулим. Ті речі, які ми сьогодні можемо робити в Інтернеті за допомогою JavaScript, який працює як на сервері, так і в браузері, було складно собі уявити ще кілька років тому.

Node.js – це серверна платформа, що призначена для створення масштабованих розподілених серверних додатків, яка використовує подієво-орієнтовану архітектуру та неблокуючу асинхронну взаємодію[3].

Головна ідея Node.js: використання неблокуючого подієво-орієнтованого вводу / виводу, щоб залишатися легким та ефективним під час роботи з додатками, що обробляють великі обсяги даних в реальному часі і функціонують на розподілених пристроях. Все це означає, що Node.js не є платформою на всі випадки життя, яка буде домінувати в світі веб-розробки. Навпаки, вона використовується лише для вирішення завдань певного типу[1]. Якщо Ваш додаток використовує тяжкі обчислення, то Вам варто відмовитися від використання Node.js, так як дані операції анулюють всі переваги даної платформи. Та якщо Ви створюєте систему, яка підтримує взаємодію з багатьма одночасними підключеннями, причому із двунаправленою взаємодією, то рано чи пізно Вам знадобиться організація асинхронного доступу. Так, саме доступу - під асинхронністю розуміють асинхронний доступ до ресурсів - файлів, сокетів, даних. За класичною схемою це відбувається так:

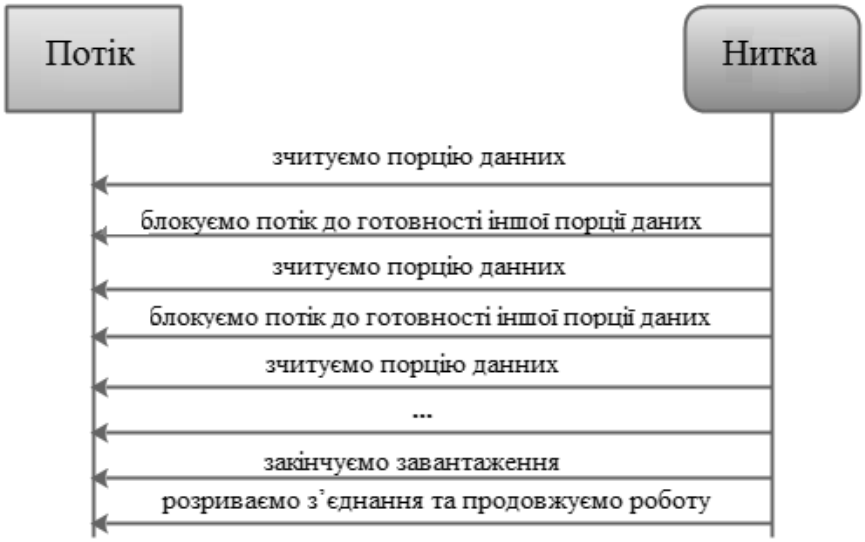


Рис. 5. Класична схема доступу до даних.

При цьому під час виконання програми виникає «блокування», яке виникає під час встановлення з'єднання з ресурсом і (особливо) під час зчитування з нього даних. Під час такого блокування потік виконання простоює, і це, безумовно, не є раціональним використанням ресурсів.

Для подолання даної проблеми була розроблена добре всім відома багатопотокова модель[4].

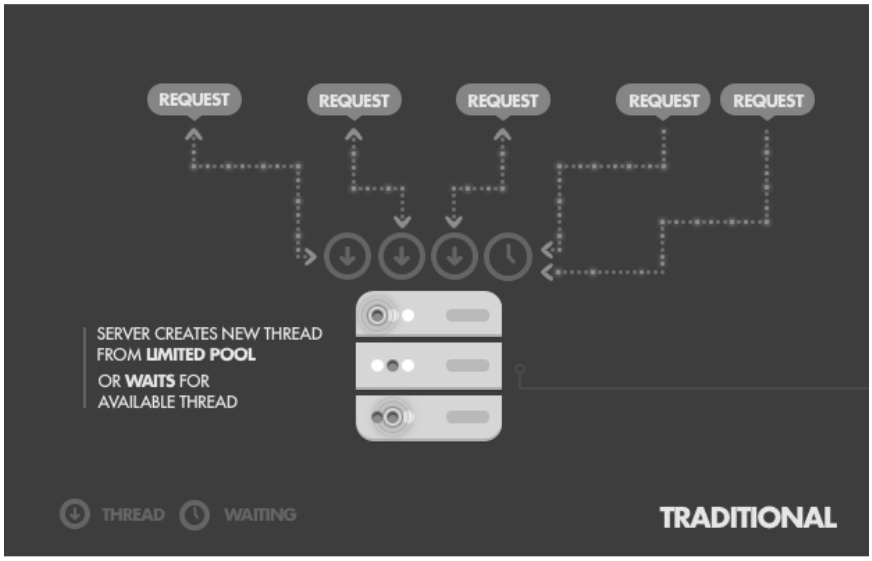


Рис. 2. Багатопотокова модель вводу / виводу.

Асинхронна модель вирішує проблеми доступу принципово по іншому. Вона побудована на циклічній черзі подій (eventloop). При виникненні деякої події (прийшов запит, відповідь від бази даних, зчитування порції даних з файлу) вона розміщується в кінець черги. Потік виконання, що обробляє цей цикл, виконує код, пов'язаний з наступним подією, і, в свою чергу, розміщує його в кінець. Це відбувається до тих пір, поки черга не спорожніє[2].

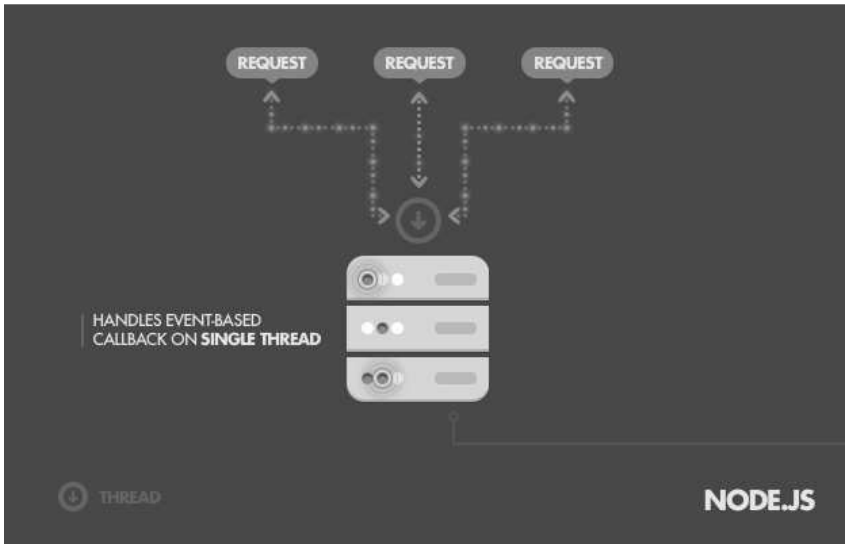


Рис. 3. Асинхронна модель вводу / виводу.

На даний момент ця технологія розвивається дуже швидко, так як має підтримку всесвітньо-відомих компаній, таких як: HBO, PayPal, Netflix, Google, Microsoft, IBM та багатьох інших. В 2015 році платформа досягла версії 4.0.0. Відразу після цієї події компанія IBM офіційно заявила про купівлю компанії StrongLoop, яка з 2013 року здійснює професійну підтримку Node.js для корпоративних клієнтів[5]. IBM вважає необхідним інтегрувати функції Node.js в свою лінійку програмних продуктів для розробки корпоративних додатків як в хмарі, так і всередині підприємства.

Node.js – це платформа, що використовується здебільшого для вирішення проблем багатокористувацьких сервісів які не потребують важких обчислень. Вона успішно застосовується для розробки веб-чатів, браузерних ігор, інформаційних порталів. В мережі можна знайти багато негативних відгуків від розробників веб-сервісів на рахунок даної технології. Здебільшого проблеми з використанням Node.js виникають тоді, коли сама платформа використовується не для тих задач, під які вона створювалась.

Література

1. Сухов К. К. Node.js. Путеводитель по технологии. – 2015. – С. 12-15.
2. Ethan Brown Web Development with Node and Express: Leveraging the JavaScript Stack. – 2014. – С. 14-16.
3. Node.js и Express как они есть [Електронний ресурс] // Издательский дом «Питер». – 2015. - Режим доступу до ресурсу: https://habrahabr.ru/company/piter/blog/265649/.
4. Why The Hell Would I Use Node.js? [Електронний ресурс] // Tomislav Caplan. – 2015. - Режим доступу до ресурсу: https://www.toptal.com/nodejs/why-the-hell-would-i-use-node-js.
5. IBM сделает платформу NodeJS стандартом корпоративной разработки [Електронний ресурс] // компания IBM. – 2015. - Режим доступу до ресурсу: https://habrahabr.ru/company/ibm/blog/266647/.

UDC 621.39

DEEP LEARNING METHODOLOGY ADAPTATION FOR HYPERSPECTRAL IMAGERY CLASSIFICATION

Piestova I.A.[1], Andreiev A.A.[2]

[1)] Scientific Centre for Aerospace Research of the Earth, Kyiv, Ukraine

[2)] Faculty of applied mathematics NTUU "KPI", Kyiv, Ukraine

E-mail: pestovai@ukr.net

Адаптація методології глибинного навчання під задачу класифікації гіперспектральних зображень

Поряд з розвитком технологій і поліпшення просторової розрізненності гіперспектральних зображень, інформація вимагає більш глибокого аналізу в зв'язку зі збільшенням кількості спостережуваних цілей. Для повного розуміння сцени тепер є обов'язковими кілька рівнів аналізу зображень. Процес глибинного навчання визначає подання та організацію декількох рівнів обробки для визначення складних відносини між гіперспектральними даними. Приведена загальна схема процесу класифікації гіперспектральних зображень з використання методології глибинного навчання. Після попередньої обробки вхідні гіперспектральні дані класифікуються в два незалежні потоки: за спектральними та за просторовими ознаками з подальшим злиттям одержаних карт ймовірностей для отримання остаточної класифікації об'єктів зображення.

Along with the technology development and the improvement of hyperspectral imagery spatial resolution, the information requires a deeper analysis due to the increased amount of observable targets. Several levels for hyperspectral imagery analysis are mandatory now for a complete scene understanding.

Representation and organization of multiple levels in order to express complex relationships among data defines a deep learning process.

Deep learning is a branch of machine learning based on a set of algorithms that attempt to model high-level abstractions in data by using multiple processing layers. For each level, models have complex structures or otherwise, composed of multiple non-linear transformations. One must be developed according to the type of information desired, namely pixel based, object based or structure based.

One of the promises of deep learning is replacing handcrafted features with efficient algorithms for unsupervised or semi-supervised feature learning and hierarchical feature extraction. Feature hierarchies are discovered considering that higher levels are formed by combining features from lower level [1].

Figure 1 describes the general outline of hyperspectral imagery classification process using deep learning methodology.

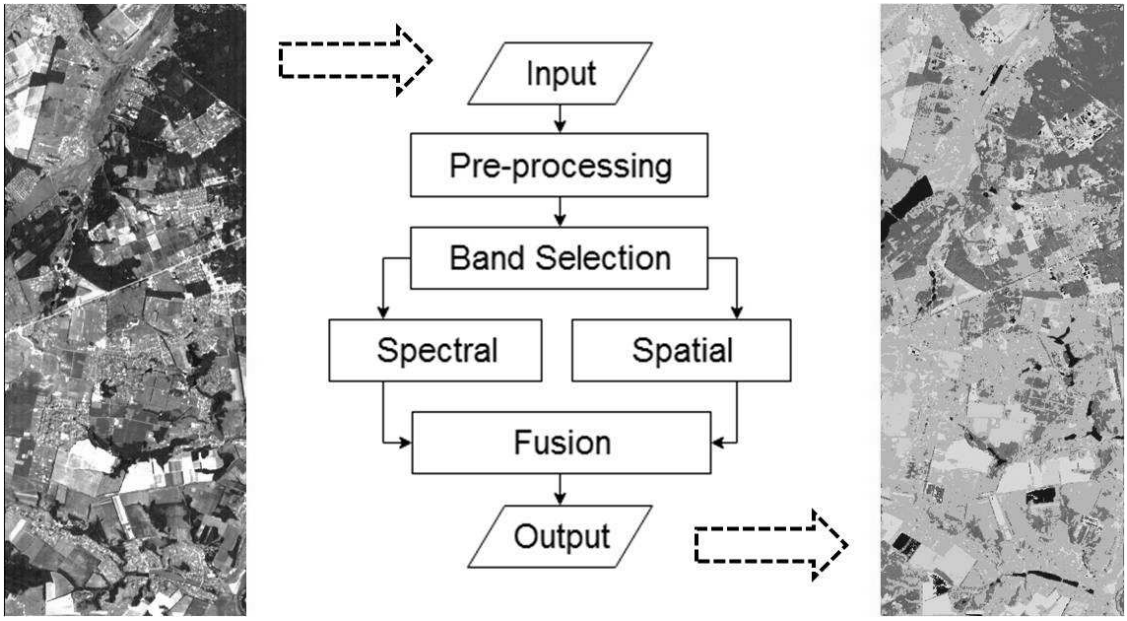


Fig.1. Deep learning data flow diagram

Input unit provides acquisition of source hyperspectral imagery.

Pre-processing unit includes radiometric and atmospheric correction and supplies by satellite imagery provider. Hyperspectral image digital numbers (DN) are converted into at-sensor spectral radiance using each-band calibration factors extracted from image metadata. Next the atmospheric correction is performed and floating-point values of the ground reflectance are obtained.

Band Selection unit makes selection of informative bands of hyperspectral image [2]. The $C(\lambda)$ informativity criterion is used for the hyperspectral imagery spectral bands selection in remote sensing applications [3]:

$$C(\lambda) = \frac{D(\lambda)}{4R^2(\lambda)} \cdot \log_2[1+\psi(\lambda)] \,, \qquad (1)$$

where $D(\lambda)$ is Kullback-Leibler divergence as a multidimensional analog of contrast for one-dimensional panchromatic image, $R(\lambda)$ is an equivalent spatial resolution of spectral bands set for current target, $\psi(\lambda)$ is an equivalent signal-to-noise ratio in target detection by multi-dimensional optical signal.

The best of spectral bands subset selection of hyperspectral image in terms of (1) criterion is an optimal search problem in hyperspectral image spectral bands combinations space [4].

Further classification of the spectral and spatial domain is performed. The first classification dataflow **Spectral** is the analysis of target features by spectral values. One detects desired targets in image for remote sensing applications. The second dataflow **Spatial** is an object-oriented classification of image targets by spatial features. Especially the Radon transform can be used to detect image targets by its shape [5] or the Hough transform can be used to detect linear patterns [6].

Both dataflows generate the corresponding intermediate probability maps for image targets. They are provided by a fundamentally different identification features.

The intermediate probability maps merging in **Fusion** unit is performed to obtain the final image targets classification. Proof of hypothesis about the target presence in image is the aim of classification outputs merging. The Bayesian inference [7] or fuzzy rules [8] can be used to restore the final probability maps.

Output unit enables the hyperspectral imagery classification availability.

References

1. *Vaduva C.* Deep learning in very high resolution remote sensing image information mining communication concept / C. Vaduva, I. Gavat, M. Datcu, // Proceedings of the 20th European Signal Processing Conference (EUSIPCO).– Bucharest: University Politehnica, 2012.– P.2506-2510.
2. *Попов М.А.* Методы оптимизации числа спектральных каналов в задачах обработки и анализа данных дистанционного зондирования Земли / М.А. Попов, С.А. Станкевич // Современные проблемы дистанционного зондирования Земли из космоса.– Вып.3.– Т.1.– М.: ИКИ РАН, 2006.– С.106-112.
3. *Станкевич С.А.* Кількісне оцінювання інформативності гіперспектральних аерокосмічних знімків при вирішенні тематичних задач дистанційного зондування Землі / С.А. Станкевич // Доповіді НАН України, 2006.– № 8.– С.53-58.
4. *Станкевич С.А.* Оптимизация состава спектральных каналов гиперспектральных аэрокосмических изображений при решении тематических задач дистанционного зондирования Земли / С.А. Станкевич // Космічна наука і технологія, 2007.– Т.13.– № 2.– С.25-28.
5. *Станкевич С.А.* Картування сільськогосподарських угідь на багатоспектральних аерокосмічних зображеннях за допомогою спеціальних просторових перетворень / С.А. Станкевич, А.В. Васько // Тези доповідей ІІ міжнародної науково-практичної конференції “Математичні моделі і методи оптимізації інновацій та інформаційно-телекомунікаціно-моніторингові технології в задачах підвищення ефективності соціоекологоекономічних систем”.– Київ: Інститут економіки та менеджменту НАУ, 2010.– С.72-75.
6. *Марков С.Ю.* Избыточное преобразование Хо / С.Ю. Марков // Информационные технологии в дешифрировании изображений: методология, модели, алгоритмы.– Киев: МО Украины, 1993.– С.22-28.
7. *Станкевич С.А.* Комплексна обробка багатоспектральних аерокосмічних зображень для виявлення сільськогосподарських угідь / С.А. Станкевич, А.В. Васько // Сучасні досягнення геодезичної науки та виробництва.– Вип.2(22).– Львів: Львівська політехніка, 2011.– С.171-175.
8. *Stankevich S.A.* Multispectral satellite imagery classification using fuzzy decision tree / S.A. Stankevich, V.G. Levashenko, E.N. Zaitseva // Communications, 2014.– Vol.16.– No.1.–P.109-113.

УДК 621.39

МОДЕЛЮВАННЯ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

Поліник С.А.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: host5x5@gmail.com

Modeling of wireless sensor networks

In the article the results of modeling of the wireless sensor networks for precision agriculture and ecological monitoring are considered. Key words: wireless sensor network, modeling.

Бездротові сенсорні мережі щороку все активніше проникають у всі галузі промисловості та сфери діяльності людини. На даний час вони широко використовуються не тільки для збору і обробки даних та керування промисловими об'єктами, але і у звичайному побуті у вигляді Інтернету речей

(Internet of Things) [1]. Бездротова сенсорна мережа (БСМ) вже перестала бути тільки об'єктом наукових досліджень і перетворюється на масовий продукт, який випускають багато виробників. Саме це зумовило появу багатьох промислових стандартів, які розробляються різними міжнародними організаціями, наприклад, Міжнародною організацією по стандартизації (ISO), Інститутом інженерів електротехніки та електроніки (IEEE), Інженерною радою Інтернету (IETF) та Міжнародним союзом електрозв'язку (ITU). Результатом роботи провідних у галузі стандартизації організацій стало сімейство стандартів IEEE 802.15.4, які визначають особливості побудови мереж з невисокою пропускною здатністю.

Існуючі та проектовані бездротові сенсорні мережі розрізняються як областями застосування, так використаними технічними рішеннями [2]. Тим не менш, можна виділити основні характеристики, які характерні більшості бездротових систем. Типова БСМ складається із великої кількості простих пристроїв або, іншими словами, вузлів для збору інформації та декількох більш складніших пристроїв, які ще називають координаторами, для обробки інформації та певного керування мережею. Кожний вузол здійснює періодичні вимірювання, первинну обробку інформації та передачу цих даних до координатора. В координаторі дані обробляються та зберігаються, а при необхідності передаються на вищий рівень або до іншої системи. Вузли можуть передавати виміряну інформацію не тільки напряму координатору, але при необхідності через інші проміжні вузли.

Слід зауважити, що специфіка БСМ передбачає можливість передачі даних від вузла до координатора через один або більше проміжних вузлів. При цьому надійність у передачі даних досягається не за рахунок встановлення надійного радіоканалу, а за рахунок підтвердження приймання кожного переданого пакету. Саме тому, для бездротових сенсорних мереж

важлива розробка необхідних протоколів мережевої маршрутизації.

Велика кількість областей застосування бездротових сенсорних мереж породжує певні проблеми, які полягають у тому, що дослідникам та розробникам мереж приходиться працювати з великою кількістю обмежень та характеристик мереж у залежності від прикладної задачі. В такому випадку моделювання є єдиним підходом, коли можна завчасно розрахувати та оцінити характеристики мережі в залежності від топології мережі, оточуючого середовища, інфраструктури без розробки реально діючих вузлів мережі.

При моделюванні протоколи, схеми, топології та навіть ідеї можуть бути оцінені у великих масштабах досить швидко і дешево. Ізза складності та тривалості налаштування БСМ широке застосування отримали різноманітні системи імітаційного моделювання мереж, які дозволяють користувачам ізолювати різні фактори лише за допомогою налаштування параметрів.

Отримання точних результатів та висновків при моделюванні не є простою задачею. Основними ключовими аспектами при моделюванні БСМ є правильність імітаційної моделі та придатність конкретних інструментів для реалізації даної моделі [4]. До фундаментальних проблем відноситься вибір між точністю, продуктивністю та масштабованістю моделі.

При виборі системи моделювання БСМ слід звернути увагу на те, що система має дозволяти:

– підвищувати ефективність розробки БСМ;

– проводити експерименти без реального розгортання сенсорної мережі;

– проводити дослідження різних режимів роботи мереж;

– зменшувати затрати на розробку та розгортання мережі в майбутньому.

Будемо вважати, що всі кінцеві вузли нашої БСМ є апаратно та програмно
ідентичні. Тому для створення моделі досить описати типовий вузол мережі, алгоритми його функціонування та взаємодії. Якщо використовувати імітаційне моделювання, то слід звернути увагу на два основних підходи до моделювання БСМ: агентноорієнтований та об'єктноорієнтований.

Об'єктно-орієнтований підхід. Кожний вузол представляється окремим класом зі своїм набором властивостей, які визначають набір методів та його поведінку. Середовище взаємодії визначається класом з параметрами, які не можуть бути описані в кожному вузлі. Ці параметри визначають цілу мережу на верхньому рівні, наприклад, кількість вузлів у мережі , протоколи передачі даних, протоколи маршрутизації тощо. Для моделювання середовища передачі даних розробляється відповідна модель радіоканалу. Крім того, для моделювання конкретної мережі слід розробити та використати додаткові моделі , наприклад, модель енергоспоживання вузла, модель явища, параметри якого зчитуються сенсором вузла тощо. Функціонування моделі вузла визначається поведінкою решти моделей, а модель бездротової сенсорної мережі визначається поведінкою моделей окремих вузлів.

Агентно-орієнтований підхід – метод моделювання, який вивчає функціонування децентралізованих агентів і як їхня робота впливає на

роботу цілої системи. На відміну від системної динаміки, в цьому підході правила для агентів визначаються індивідуально і правила функціонування цілої системи є результатом спільної діяльності багатьох агентів. При такому моделюванні використовується підхід "знизу вверх". Агентноорієнтований підхід включає у себе елементи теорії ігор, складних систем, багатоагентних систем та еволюційного програмування. Також застосовується метод Монте-Карло, теорія ймовірності та математична статистика.

Агентноорієнтоване моделювання бездротових мереж у деякій мірі являє собою підвид імітаційного моделювання, в якому основну увагу приділено дослідженню стану глобальної системи в залежності від поведінки агентів, які є компонентами системи. У випадку бездротових сенсорних мереж цей підхід є доцільним, так як вузли мережі розподілені на великій території, активно взаємодіють з навколишнім середовищем та сусідніми вузлами, а поведінка та технічні характеристики окремого вузла безпосередньо впливають на функціонування та продуктивність цілої мережі.

Враховуючи вище вказане, можна зробити висновок, що вибір інструменту для моделювання БСМ, який би максимально точно враховував всі фактори та обмеження, є складною задачею. На даний час існує кілька програмних засобів, які дозволяють моделювати бездротові сенсорні мережі з урахуванням багатьох факторів. Найбільш відомими є Anylogic, TOSSIM, OPNET Modeler, Network Simulator (NS, NS2, NS3), GloMoSim, Worldsens, NetSim, OMNeT++, Castalia.

Серед вказаних програмних інструментів є як платні, так і безплатні варіанти.

Література

1. *Recommendation* Y.2060 "Overview of the Internet of things" // International Telecommunication Union Telecommunication Standardization Sector, 2012.
2. *Shorey R., Ananda A., Mun Choon Chan, Wei Tsang Ooi*. Mobile, wireless, and sensor networks: technology, applications, and future directions // USA: A John Wiley & Sons, Inc. 2011. – 430p.
3. *Kryvonos Yu., Romanov V., Wojcik W., Galelyuka I., Voronenko A.* Application of wireless technologies in agriculture, ecological monitoring and defense // Proceeding of the 8th IEEE International conference on "Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications", IDAACS'2011. – Warsaw, Poland. – 2015, September 24–26.
4. *Борисенко А.С., Галкин П.В.* Адекватность моделей беспроводных сенсорных сетей в средах имитационного моделирования // Восточно-Европейский журнал передовых техноло гий. – 2013. – № 4/ 9 (64). – С. 52–55.
5. *https*://omnetpp.org.
6. *http*://castalia.forge.nicta.com.au/index.php/en/index.html.
7. *Грудинская Г.П.* Распространение радиоволн. – М.: Высшая школа, 1975. – 280 с.
8. *Шабунин С.Н., Лесная Л.Л.* Распространение радиоволн в мобильной связи: Методическое пособие. – Екатеринбург: УГТУ, 2000. – 38 с.
9. *Pottie G.J., Kaiser W.J.* Wireless integrated network sensors // Commun. ACM, 43(5):51– 58. – 2000.

УДК 621.382

МЕТОД ПІДВИЩЕННЯ ПРОПУСКНОЇ ЗДАТНОСТІ МОБІЛЬНИХ СЕНСОРНИХ МЕРЕЖ З ТЕЛЕКОМУНІКАЦІЙНИМИ АЕРОПЛАТФОРМАМИ

Прищепа Т.О., Лисенко О.І.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: its_tk@ukr.net

Methods for improving capacity of mobile sensor networks with telecommunications aero platforms

We consider the application of sensor networks with mobile telecommunications aeroplatform (TA) in terms of emergency response. A method forincreasing the capacity of the mobile sensor networks and in the rapid and unexpectedmovement of mobile sensors.

В умовах пошкодження або відсутності наземної інфраструктури (різного роду надзвичайні ситуації) широкого використання набувають мобільні сенсорні мережі (МСМ).[1,6] Мобільні сенсори можуть вільно пересуватися в заданому районі і з'єднуватися між собою безпосередньо - в зоні видимості, або з ретрансляцією пакетів через сусідні вузли (якщо ці вузли виконують функцію маршрутизації), утворюючи, таким чином, багатоланкові мережі довільної структури. Збільшити зону покриття МСМ можливо шляхом ієрархічної просторової організації мережі з застосуванням телекомунікаційних аероплатформ різних рівнів, що виконують роль ретрансляторів, поєднуючи між собою віддалених абонентів. Особливо актуально застосування телекомунікаційних аероплатформ на основі мініатюрних безпілотних літальних апаратів (БПЛА), наприклад, квадрокоптера, що є більш оперативним і економічним на відміну від використання великих аероплатформ.

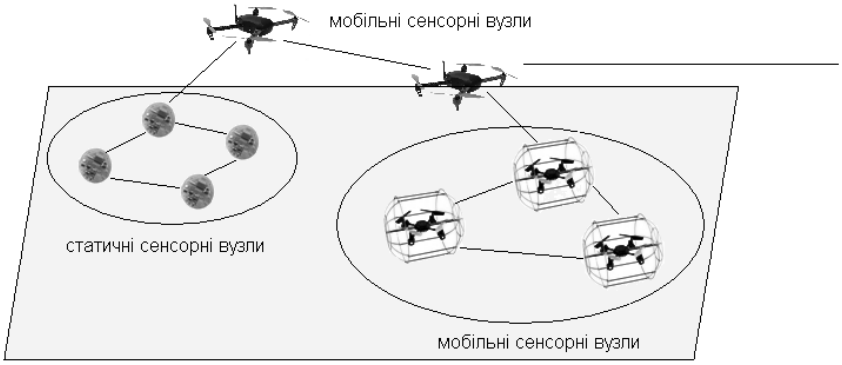


Рис. 1 Приклад МСМ.

Топологія таких мобільних радіомереж носить динамічний характер і постійно розвивається, а значить, вимагає ефективної системи управління (СУ), яка буде швидко реагувати на структурні і функціональні зміни, забезпечуючи ті чи інші цілі управління, а саме:

- забезпечення зв'язності (структурної надійності);
- якість маршрутів передачі даних між абонентами (QoS);
- підвищення пропускної спроможності мережі і ін.

Керуючими параметрами в даному випадку можуть виступати потужність передавачів, навантаження, взаємне положення вузлів і ін. Недостатньо вирішеною на сьогодні завдання оптимального оперативного розміщення безлічі телекомунікаційних аероплатформ для підвищення пропускної здатності мережі з одночасним забезпеченням структурно-функціональної зв'язності мобільних сенсорів. Запропоновані на сьогодні методи, закладені в СУ топологією (Місцем розташування), вирішують лише часткові завдання забезпечення геометричній зв'язності роз'єднаних компонентів мережі, без урахування обмеження ємності канальних ресурсів, розподілу навантаження і обслуговування пакетів у вузлах мережі. Також більшість методів вирішують тільки статичні завдання, не враховуючи характер мобільності сенсорів і маневреність, отже, підлягають вдосконаленню. Існуючі методи планування наземних радіомереж теж ефективні, так як мають велику складність і час обчислення, що не дозволяє відпрацьовувати отримані рішення в режимі реального часу. В зв'язку з цим, підвищення пропускної спроможності мобільних сенсорних мереж з телекомунікаційними аероплатформ з одночасним забезпеченням структурно-функціональної зв'язності мобільних сенсорів в умовах їх швидкого і непередбачуваного переміщення є актуальним завданням. [2]

Постановка задачі. Нехай задані: множина мобільних абонентів $V_i, i = \overline{1,N}$, де N - кількість мобільних абонентів (МА), розосереджених в деякому районі; множина БПЛА $B_j, j = \overline{1,K}$, де K - кількість БПЛА; R - радіус зони обслуговування кожного БПЛА, м; D^0 (P^0) - радіус (потужність) передачі кожного БПЛА. [4] Кожен МА мережі в момент часу t описується сукупністю параметрів: координатами розміщення і швидкістю руху (x_i, y_i), S_i, $i = \overline{1,N}$; висотою щодо земної поверхні h (будемо вважати, що h=0); радіусом (потужністю) передачі d^0 (p^0); маршрутної таблиці найкоротших маршрутів $П_i$.

Тоді постановку задачі можна сформулювати наступним чином: знайти в режимі реального часу такий управлінський вплив C_T (координати розміщення множини БПЛА в просторі (x_{0j}, y_{0j}, z_{0j}), S_{0j}, $= \overline{1,K}$, що визначають матрицю зв'язності A^j), яке забезпечить максимум цільової функції зв'язності.

$$W = U^з \longrightarrow \max A^j \qquad (1)$$

управління Метод топологією мережі БПЛА для підвищення структурно-інформаційної зв'язності МСМ Управління топологією мережі БПЛА включає в себе наступні етапи: планування, розгортання, оперативне управління.

Етап планування здійснюється центром управління мережі БПЛА. Він містить в собі:

1. Планування топології мережі БПЛА (знаходження необхідного кількості БЛА, визначення їх початкового місця розташування або переміщення в просторі), що реалізує певні цілі управління (підвищення структурної та / або інформаційної зв'язності мережі), виходячи з вимог до параметрів мережі та вимог щодо передачі трафіку.

2. Розподіл ресурсів (апаратурних, частотних, енергетичних, просторових) мережі БПЛА, вибір конкретних параметрів і режимів роботи технічних засобів (методів і алгоритмів управління).

Етап розгортання полягає в запуску заданої кількості БПЛА і управлінні їх польотом в задані райони баражування (Місця їх початкового розташування). При цьому завдання етапу розгортання (перепланування топології) мережі БПЛА можуть виконуватися і на етапі оперативного управління при значних змінах мережі (Її пошкодження, введенні нових угруповань вузлів і ін.). Контроль за польотом БПЛА і роботою його бортових систем здійснюється з центру управління мережею.

На етапі оперативного управління за прийнятими критеріями ефективності постійно оцінюється стан мережі, і приймаються заходи (відповідно до плану і реальну обстановку) по утриманню показників ефективності функціонування (пропускної спроможності) в заданих межах або їх оптимізації. завдання оперативного управління (на відміну від завдань планування) вирішуються змішаним способом (централізовано / децентралізовано) в режимі реального часу.[3]

В докладі наводиться відповідний огляд поточних досліджень поставленої задачі. Надається метод підвищення пропускної здатності МСМ з телекомунікаційними аероплатформами.

Література

1. Прищепа Т.О. Безпроводові сенсорні мережі із мобільними сенсорами / Т.О. Прищепа, О.І. Лисенко // 9-а міжнар. наук.-техн. конф., 21-25 квітня 2015р. : тези доп. – К., 2015. – С. 378-381.
2. Прищепа Т.О. Застосування сенсорних телекомунікаційних систем в умовах надзвичайних ситуацій / Т.О. Прищепа // Науковий вісник Академії муніципального управління. Збірник наукових праць. Серія «Техніка» – 2014. – Вип. 7. – С. 153-157.
3. Прищепа Т.О. Методи оцінки границь досяжності значень показника якості телекомунікаційної системи зони лиха в умовах деструктивних впливів / Т.О. Прищепа // Науковий вісник Академії муніципального управління. Збірник наукових праць. Серія «Техніка» – 2013. – Вип. 6. – С. 129-141.
4. Лысенко А. И. Метод оптимального управления топологией сети беспилотных летательных аппаратов / А.И.Лысенко, С.В.Валуйский, Т.А.Прищепа //СВЧ- техника и телекоммуникационные технологии(КрыМиКо '2010): 20-я междунар. крымская конф., 13-17 сен. 2010г. : материалы конф. – Севастополь, 2010. – Т.1. – С. 333–334.
5. Sensor networks: evolution, opportunities, and challenges / CY Chong, SP Kumar - Proceedings of the IEEE, 2003
6. Introduction to wireless and mobile systems / D Agrawal, QA Zeng - 2015

УДК 621.396.4

ВИКОРИСТАННЯ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ УПРАВЛІННЯ В СЕНСОРНИХ МЕРЕЖАХ ІЗ МОБІЛЬНИМИ СЕНСОРАМИ

Романюк А.В., Лисенко О.І.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: anton.romaniuk@gmail.com

Using intelligent control systems in sensor wireless networks with mobile sensors

This article describes using of intelligent control systems in sensor networks with mobile sensors. Described basic methods of intelligent control and analyzed their weaknesses, proposed the architectural scheme of intelligence control system.

Безпроводові сенсорні мережі з мобільними сенсорами (БСММС) належать на самоорганізуючих радіомереж, складаються з невеликої кількості простих автономних *мобільних* сенсорних вузлів, що містять сенсор, процесор, систему передачі даних, джерело енергії. Ці вузли поширюються на території для виконання завдання дослідження певного явища. На даний момент вони успішно застосовуються в промисловості, сільському господарстві, військовій сфері.

Системи управління (СУ) таких мереж інтенсивно розвиваються в напрямку інтелектуалізації, при цьому істотно змінюється технологія прийняття управлінських рішень. Реалізація всіх етапів управління БСМ з використанням методів (моделей) інтелектуального управління вузловими та мережевими ресурсами, а також відповідних програмних та апаратних засобів, дозволить: забезпечити збір і обробку необхідних (мінімальних) обсягів службової інформації про стан БСММС; ідентифікувати стан БСММС та здійснювати його прогнозування з урахуванням високої динаміки зміни топології мережі та інших параметрів її функціонування; визначати вузлові та мережеві цільові функції управління щодо оптимізації процесу обслуговування трафіка; визначати стратегії та способи досягнення цільових функцій; координувати управлінські рішення, що приймаються інтелектуальними СУ вузлів (на маршруті передачі чи інформаційному напрямку) в умовах децентралізованого управління БСМ, поповнювати бази знань вузлових систем управління новими правилами з використанням методів самонавчання.

Відповідно, під терміном *інтелектуальна система управління*(ІСУ) БСМС будемо розуміти множину взаємодіючих у процесі передачі інформації вузлових інтелектуальних СУ, в основі яких знаходиться математичне (програмне) забезпечення, яке здатне реалізувати функції інтелектуального управління БСМ, в умовах її параметричної та структурної невизначеності, шляхом збору і перетворення службової інформації про стан БСМС у знання про цілі та параметри функціонування мобільних вузлів для реалізації рішень щодо якісного обслуговуванню трафіка, а також забезпечити спроможність вузлових інтелектуальних СУ до навчання на власному досвіді (самонавчання).

На сьогоднішній день інтелектуальні алгоритми в ІСУ реалізують тільки окремі функції або працюють на окремих рівнях в системі управління БСМС.

Наприклад, в [2, 3] запропоновано алгоритми маршрутизації, засновані на мурашиному алгоритмі і ройовому інтелекті. Вони вирішують проблеми масштабованості, але вимагають маршрутизацію від джерела, що потребує використання пристроїв пам'яті і обчислювальної потужності на сенсорних вузлах. Початково розроблені для мереж MANET, такі алгоритми потребують значного вдосконалення в плані енергозбереження для БСММС.

В [4] запропоновано ІСУ з алгоритмом, заснований на нечіткій логіці, який використовує контролери QoS (контролери якості обслуговування). Даний алгоритм зменшує затримки и вірогідність передачі повідомлень за допомогою присвоєння значень QoS кожному пакету, який розраховується нечітким планувальником. Але такий метод значно підвищує обчислювальні вимоги до мережі, що знижує час життя мережі. Дані ІСУ також були розроблені для мереж MANET, використання в БСМС потребує значних вдосконалень механізмів енергоефективності.

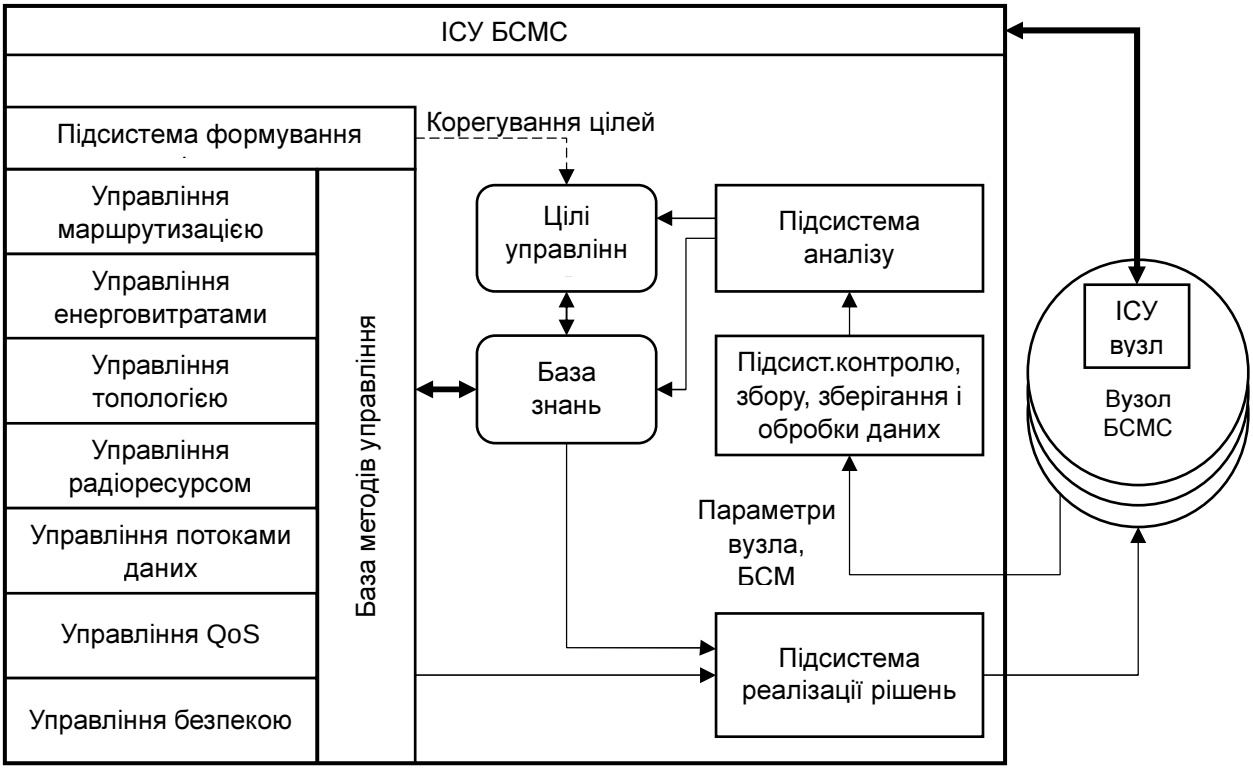


Рис. 1. Приклад моделі ІСУ.

Таким чином, існуючі методи інтелектуального управління сенсорних мереж реалізують тільки окремі функції системи управління і вимагають значних обчислювальних потужностей. Для вирішення поставленої проблеми можлива побудова ІСУ за наступною схемою (рис. 1).

Важливо зазначити, що головна архітектурна особливість [5], яка відрізняє ІСУ від побудованої за традиційною (СУ без інтелектуальних методів управління) схемою, пов'язана з підключенням механізмів зберігання й обробки знань (блок «база знань») для реалізації здатності виконувати необхідні функції в умовах невизначеності (неповноти інформації) при випадковому характері зовнішніх впливів. В базі знань міститься інформація про принципи побудови системи управління та мету її

функціонування, специфіку використання різних методів управління, а також особливості функціонування підсистеми реалізації рішень та самого об’єкту управління. Крім того, до складу системи управління, у разі необхідності, може входити підсистема поповнення знань та навчання, яка забезпечує узагальнення накопиченого досвіду і, таким чином, поповнює базу новими знаннями.

Підсистема контролю, збору, обробки і зберігання даних призначена для вимірювання контрольованих параметрів мобільних вузлів та радіомережі в цілому. Звичайно, знання повної інформації про мережу дозволяє приймати більш обґрунтовані рішення, однак приводить до значного зростання службового трафіка в умовах динаміки топології і вхідного навантаження.

Підсистема формування рішень побудована за принципом функціональності управління, який передбачає об’єднання функцій системи управління у відносно незалежні групи, що дозволяє здійснити декомпозицію управління мережею на підсистеми (що значно спрощує задачу розробки математичного забезпечення управління).

За проведеним аналізом випливає задача розробки методу інтелектуального управління сенсорною мережею з мобільними сенсорами, що дозволить мінімізувати об’єм службового трафіку, і приймати рішення, близькі до оптимальних за невеликий проміжок часу. Виникає задача мультикритеріальної оптимізації для забезпечення ефективного використання енергоресурсів, низького часу прийняття рішення, високої ефективності використання обчислювальних ресурсів. Подальші дослідження будуть містить вищеописаний метод та імітаційну модель для підтвердження результатів аналізу.

Література

1. Міночкін А.І., Романюк В.А. Методологія управління тактичними сенсорними мережами // IV Науково-технічна конференція ВІТІ «Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення». – К.: ВІТІ НТУУ “КПІ”. – 2008. – С. 15 – 25.
2. V. Raghavendran, G. Naga Satish, P. Suresh Varma. Intelligent Routing Techniques for Mobile Ad hoc Networks using Swarm Intelligence // I.J. Intelligent Systems and Applications, 2013, 01, pp. 81-89
3. Rajesh war Singh, D. K. Singh, Lalan Kumar. Swarm intelligence based approach for routing in mobile Ad Hoc networks // International Journal of Scienceand Technology Education Research Vol. 1(7), pp. 147 – 153, December 2010
4. B. Sun, C. Gui, Q. Zhang, H. Chen. Fuzzy Controller Based QoS Routing Algorithm with a Multi class Scheme for MANET // Int. J. of Computers, Communications & Control, ISSN 1841-9836, E-ISSN 1841-9844 Vol. IV (2009), No. 4, pp. 427-438
5. Романюк В.А. Інтелектуальні мобільні радіомережі // V науково-технічна конференція ВІТІ «Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення» / – К.: ВІТІ НТУУ «КПІ», 2010. – С. 28 – 36.

УДК 351.321

ПОКРИТТЯ В БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ

Семініченко В. В., Алєксєєва І.В.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
Email: viktoriyaseminichenko@gmail.com

Coverage in wireless sensor networks

In this work coverage with connectivity properties in large wireless sensor networks is studied. Three classes are considered: full coverage, partial coverage, and constrained coverage. Two simple network topologies are outlined. The surveillance performance and deployment cost for networks with different coverage with connectivity criteria is compared.

Останні досягнення в галузі мікроелектроніки та цифрової обробки сигналів дозволили розгортання великих безпроводових сенсорних мереж [1]. Безпроводові сенсорні мережі можуть бути розгорнуті в районах без підтримки інфраструктури, в суворих умовах[2].

Розглянуто безпроводову сенсорну мережу, де датчики мають здатність як зондування і комунікаційні можливості. Покриття та підключення основні вимоги в безпроводової сенсорної мережі. Метою такої мережі є збір даних, та повідомлення отриманої інформацію до центру.

Покриття можна класифікувати наступним чином: повне, часткове і обмежене [3]. Точка вважається покритою, якщо події, що сталася в цьому місці, можуть бути виявлені за допомогою одного або декількох датчиків. Нехай Rs - діапазон чутливості датчика. Точка є покритою, якщо відстань від неї до хоча б одного датчика не більш ніж Rs. Два датчика безпосередньо пов'язані, якщо відстань між ними менше дальності зв'язку, Rc. Було припущено, що Rs = Rc/2.

На рисунку 1, показано результат в різних щільності в квадраті з L = 100, і Rc = 1. Розмір поля A = L^2 = 10000. ε= -0.1,0,0.1,0.3. Найбільший підключений компонент позначений чорним, а різні рівні сірого показують інші компоненти. Випадок, коли ε = -0,1 відповідає рівню нижче критичного, коли розмір кожного компонента обмежений з ймовірністю 1, L прямує до нескінченності. Є багато дрібних скупчень, які не пов'язані один з одним.

Випадок, коли $\varepsilon = 0$ відповідає критичному випадку. Випадки, коли $\varepsilon = 0.1,0.3$ відповідають надкритичному випадку. Існує один гігантський компонент, який включає більшість з вузлів. Чим більше величина ε, тим більше число вузлів, включених в цей компоненти. При $\varepsilon = 0,3$ більшість території вкрита гігантським компонентом.

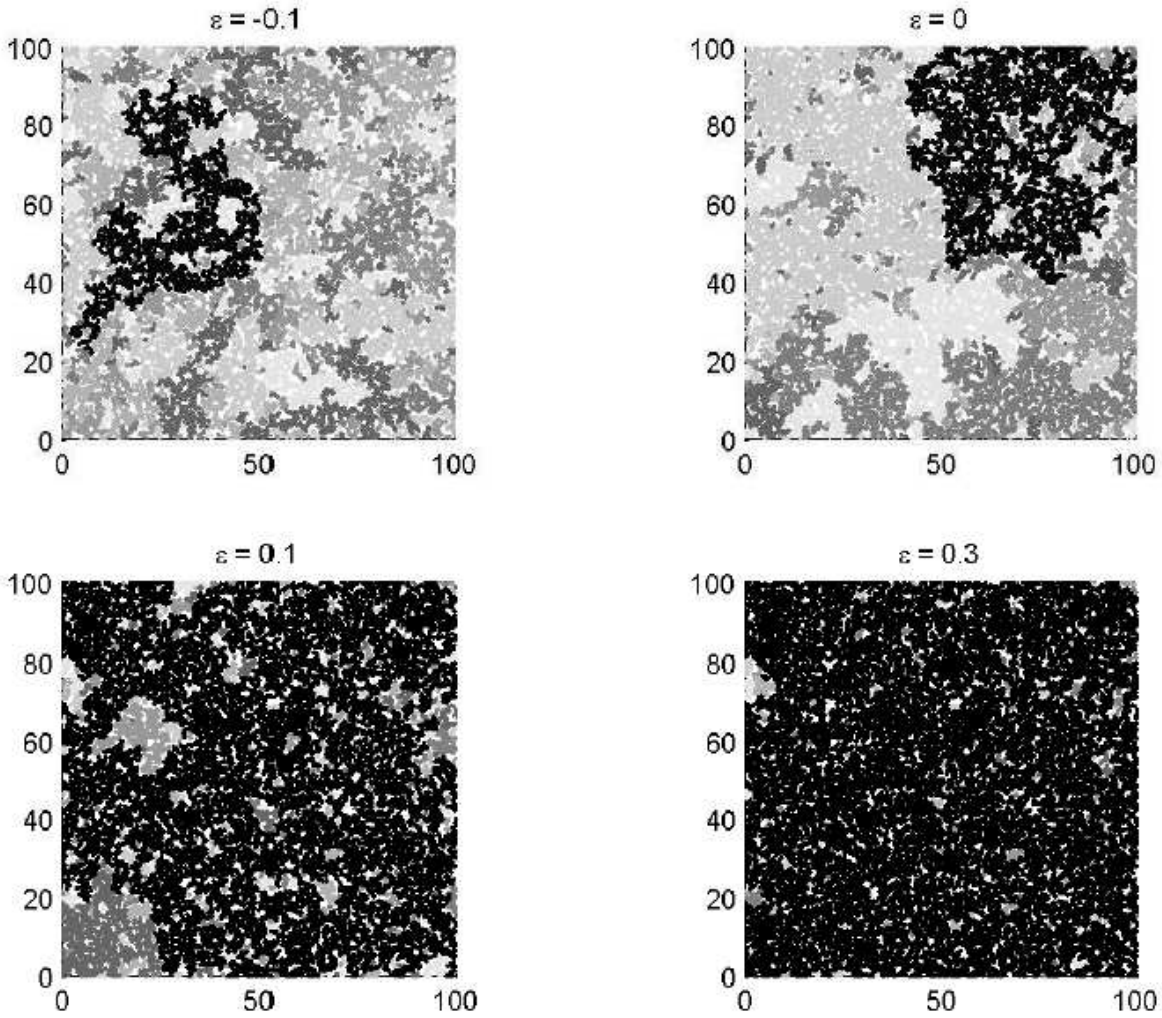


Рис. 1. Властивості фільтрації прирізних значеннях ε.

Повне покриття забезпечує найкращу якість спостереження на найвищою ціною. Коли деякі датчики вичерпали енергію або не працювати, повне покриття може змінитися на часткове [4]. У мережі з частковим покриттям, більшість площі покрито з можливістю підключення. Центр обробки інформації може виявити події в більшості випадків. Коли щільність датчиків стає нижче критичної, більшість мережі від'єднується хоча центр

може бути пов'язаний з невеликою кількістю датчиків. Властивість зв'язності пов'язана з щільністю, коли вона близька до критичної. Для того, щоб забезпечити кращу відмовостійкість, можна зробити $\varepsilon \geq 0.1$. Обмежене покриття відрізняється від попередніх двох, тому що присутня деякий ступінь контролю над розміщенням датчика. Уздовж траєкторії випадковим чином розміщуються сенсори.

ВИСНОВОК. Пропонується дві прості мережеві топології. Основна перевага обмеженого покриття є його гнучкість: кількість необхідних датчиків залежить від необхідної точності спостереження. Іншими словами, коли є багато датчиків, мережа може бути розгорнута для надання інформації спостереження високої якості. Коли кількість доступних датчиків обмежена, мережа збору інформації може бути розгорнута.

Можна зробити висновок щодо вибору покриття у вигляді таблиці:

Таблиця 1. Порівняння видів покриття.

Покриття	***Характеристика***	***Ціна***
Повне	Найкраще	Найвища
Часткове	Добре	Середня
Обмежене	Залежить від точності	Залежить від точності

Література

1. B. Wang, W. Wang, V. Srinivasan, and K. C. Chuah, “Information coverage for wireless sensor networks”, *IEEE Communication Letters,* vol. 9, no. 11, 2005.
2. Wei Wang, Vikram Srinivasan, Bang Wang, and Kee-Chaing Chua, “Coverage for target localization in wireless sensor networks”, in *IPSN ’06: Proceedings of the fifth international conference on Information processing in sensor networks,* New York, NY, USA, 2006, pp. 118125, ACM Press.
3. S. Megerian, F. Koushanfar, M. Potkonjak, and M. Srivastava, “Worst and best-case coverage in sensor networks”, *IEEE Transactions on Mobile Computing*, vol. 4, no. 1, 2005.
4. X. Wang, G. Xing, Y. Zhang, C. Lu, R. Pless, and C. Gill, “Integrated coverage and connectivity configuration in wireless sensor networks”, in *ACM SenSys’03*, 2003.

УДК 621.391

МАРШРУТИЗАЦІЯ З ГАРАНТОВАНОЮ ДОСТАВКОЮ В 3D БЕЗПРОВІДНИХ СЕНСОРНИХ МЕРЕЖАХ

Стрихалюк Б.М., Климаш Ю.В.
Інститут телекомунікацій, радіоелектроніки та електронної техніки
Національний університет «Львівська політехніка», Україна
E-mail: bogdan_str@ukr.net, mklimash@polynet.lviv.ua

Routing with guaranteed delivery in 3D wireless sensor networks

With both computational complexity and storage space bounded by a small constant, greedy routing is recognized as an appealing approach to support scalable routing in wireless sensor networks. In this research we develop decentralized solutions to achieve greedy routing in 3D sensor networks. Our proposed approach is based on a unit tetrahedron cell (UTC) mesh structure. We propose a distributed algorithm to realize volumetric harmonic mapping of the UTC mesh under spherical boundary condition.

Різні підходи були розроблені для вирішення проблеми локального мінімуму в 2D - мережах, з основним акцентом на межах. Серед всіх алгоритмів маршрутизації, обговорюваних в літературі для 3D сенсорних мереж, Random - Walk є єдиним алгоритмом жадібної маршрутизації з постійно - обмеженим зберіганням і складністю обчислень. Пропоноване нами рішення засноване на комірці тетраедра сітчастої структури. Ми пропонуємо розподілений алгоритм для реалізації об'ємного гармонійного відображення сітки при сферичній граничній умові. Це схема один – до - одного, що дає віртуальні координати для кожного вузла в мережі. Оскільки межа зіставлена з сферою, жадібна маршрутизація на основі вузлів, є завжди успішною. Наскільки нам відомо, це є першою роботою, яка реалізує дійсно детерміновану жадібну маршрутизацію з постійно - обмеженим зберіганням і обчисленнями в 3D сенсорних мережах.

Ми представляємо безпровідну сенсорну мережу за допомогою графа $G(V,E)$, де вершини V позначають вузли датчиків і ребра E позначають лінії зв'язку в мережі.

Простий алгоритм використовується для створення сітки комірок тетраедра, яка починається з будь - якого довільного тетраедра. При видаленні всіх ребер, які перетинають цей тетраедр, алгоритм дає блок комірок тетраедра , що позначається $БКТ(A,B,C,D)$. Далі алгоритм розширює його, щоб сформувати інші БКТ-с. Грунтуючись на кожній грані $БКТ(A,B,C,D)$, такі як $Face(A,B,C)$, алгоритм шукає загальних сусідів вузлів A,B,C. Нехай E такий загальний сусід. Вершини A,B,C,E утворюють діючий БКТ, тільки якщо він не перетинається з існуючим БКТ-с, не містить будь-яких інших вузлів. Кілька таких вузлів, як E може існувати, і алгоритм довільно обирає один з них, щоб сформувати новий БКТ. Алгоритм повторює цю процедуру доки буде сформовано всі можливі БКТ.

Ми припускаємо, що вузол може створити локальну систему координат за допомогою локальної інформації про відстані за допомогою стандартних

методів [1-3].

Наша мета полягає в тому, щоб дозволити жадібну маршрутизацію від будь-якого джерела до будь - якого вузла призначення в тій чи іншій сенсорній мережі. Більш конкретно, ми прагнемо відобразити довільну мережу 3D сенсора до жадібно досяжної мережі, як визначено нижче: Визначення 1. Мережа називається жадібно досяжною мережею, якщо кожні два вузла в мережі є жадібно досяжними один одному.

Об'ємне вкладення – це процес обчислення схеми між вихідними об'ємними даними і канонічною областю в R^3.

Для обчислення обсяг моделюється як хмари точок або частина лінійно тетраедної сітки.

$$M = (T, F, E, B, C) \tag{1}$$

де T, F, E, B є множинами тетраедра, триангулярних граней, ребер і вершин в сітці, C – описує зв'язок між ними.

Об'ємне вкладення призначає набір 3D координат кожної вершини в об'ємних даних. Значення функції для довільної точки в об'ємі визначається як інтерполяції значень на чотирьох вершинах, що обводить тетраедр, викликаючи кусочно - лінійне відображення з вихідної об'ємної сітки M до канонічного домену N. Домен N є підмножиною R^3, і в ідеалі повинен мати правильну форму. В нашому випадку, канонічний домен є суцільна куля, щоб підтримати жадібну маршрутизацію.

Наша мета полягає в побудові віртуальних координат для 3D сенсорної мережі, щоб підтримувати успішну жадібну маршрутизацію.

Віртуальні координати повинні бути відповідні один – до - одного до вузлів датчиків. З цією метою ми вдаємося до об'ємного гармонійного відображення (ОБВ) при сферичній граничній умові. У загальному випадку, функція F є гармонійна, якщо вона задовольняє рівняння Лапласа $\Delta f = 0$.

Для краю e_{ij}, що з'єднує вершини v_i та v_j, вага краю k_{ij} є реальною величиною і визначається наступним чином:

$$k_{ij} = \frac{1}{t}\sum_{m=1} l_m \cot \theta_m, \tag{2}$$

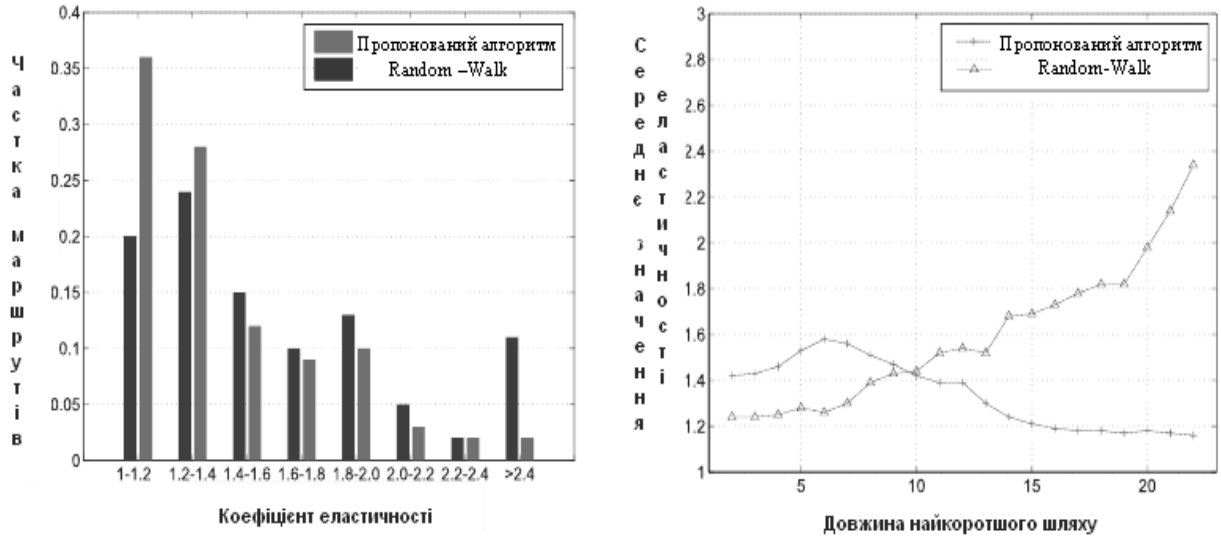
де t - прилеглий тетраедр, θ_m - двогранний кут, l_m - довжина краю до e_{ij} в сітці БКТ.

Ми побудуємо об'ємне гармонійне відображення з методу теплового потоку таким чином, що сітка БТК гомеоморфно (один до одного) зіставлена з суцільною кулею тетраедра в R^3.

Розглянемо передачу пакета між вузлами S і D. Коли пакет не може знайти шлях до вузла D, він повинен прийти до кордону сфери. Таким чином, на основі жадібна маршрутизація на основі вузла застосовується для переміщення пакета через порожнечу. Кожен раз, коли D стає досяжним, жадібна маршрутизація на основі зовнішньої сторони застосовується знову. Такий процес триває доки пакет не досягне свого вузла призначення.

В запропонованому алгоритмі використовується розподілене сферичне і об'ємне гармонічне відображення. Після відображення, кожен вузол має свої

власні віртуальні координати в 3D - просторі. Було здійснено моделювання пропонованого алгоритму в 3D сенсорних мережах. Фактор елатичності маршруту є відношенням фактичної довжини шляху до найкоротшої. Випадковим чином було вибрано 10000 пар вузлів для розрахунку середнього коефіцієнта еластичності.



(а) (б)

Рис.1. а) Розподіл фактора еластичності, б) Вплив довжини шляху.

Більшість шляхів маршрутизації в рамках запропонованого алгоритму мають низький коефіцієнт еластичності. Наприклад, 70% маршрутів мають коефіцієнт еластичності менше, ніж 1,4. В той час як розподіл після Random – Walk має значний зсув в праву сторону - близько 20% маршрутів, в яких коефіцієнт еластичності 2.0 або вище. (рис.1(а)).

З рис. 1 (б), бачимо, що з збільшенням фактичної довжини шляху між джерелом і пунктом призначення, коефіцієнт еластичності зменшується за нашою схемою.

В роботі було досліджено рішення для досягнення жадібної маршрутизації в 3D сенсорних мережах. Запропонований підхід заснований на блоці комірок тетраедра сіткової структури.

Запропоновано розподілений алгоритм для реалізації об'ємного гармонійного відображення сітки БКТ при сферичній граничній умові. Оскільки межа зіставлена з сферою, жадібна маршрутизації на основі вузлів завжди успішна.

Література

1. X. Bai, C. Zhang, D. Xuan, J. Teng, and W. Jia,“Low-Connectivity and Full-Coverage Three Dimensional Networks,” in Proc. of MobiHOC, pp. 145–154, 2009.
2. X. Bai, C. Zhang, D. Xuan, and W. Jia, “Full-Coverage and K-Connectivity (K=14, 6) Three Dimensional Networks,” in Proc. of INFOCOM, pp. 388–396, 2009.
3. C. Liu and J. Wu, “Efficient Geometric Routing in Three Dimensional Ad Hoc Networks,” in Proc. of INFOCOM,pp. 2751–2755, 2009.

УДК 621.396

НАДІЙНИЙ ПРОТОКОЛ МАРШРУТИЗАЦІЇ ДЛЯ СЕНСОРНОЇ МЕРЕЖІ

Тарасюк В. О.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: vika_tarasiuk008@mail.ru

Reliable routing protocol for sensor network

The approach to improve reliability based on automatic re-sending data through the cooperation between nodes. Each node has a small buffer for caching packets. If the neighboring node detects packet loss it can retransmit packet using a buffer.

У традиційних бездротових мережах широкомовний характер каналів вважається серйозною проблемою. Загальна продуктивність мережі може бути поліпшена, якщо «підслухана» інформація правильно перенаправляється оточуючими вузлами. Поліпшення, викликане за рахунок використання співпраці вузлів в бездротових мережах, може бути отримане з точки зору підвищення надійності, зниження енергоспоживання, або навіть збільшеної дальності покриття. Співпрацю було використано, щоб подолати проблеми завмирання сигналу і підвищити якість бездротового зв'язку.

Для зменшення кількості втрачених пакетів пропонується змінити метод повторної передачі даних. Передача відбуватиметься наступним чином: джерело передає кадр до місця призначення, і, у разі помилки, вузол ретрансляції ретранслює кадр, таким чином забезпечуючи систему з кооперативною різноманітністю. Цього можна досягнути завдяки кешуванню «підслуханих» сусідніми вузлами даних. Якщо відбуватиметься втрата пакетів, сусідні вузли пересилатимуть дані, які вони раніше «підслухали». Таким чином, більше не потрібна повторна передача вузлом, який першим відправив пакет.

Запропоновано три різні кооперативні схеми кешування (дані, шляхи і гібридне кешування).

У даному протоколі зберігаються припущення, що безпровідна мережа датчиків щільно розгорнута випадковим чином; пакети генеруються

випадково і пересилаються крок за кроком на приймальний вузол. Якщо шлях 1-2 на рисунку 1 зазнає невдачі через глибоке завмирання, то вузол 2 втратить пакет. Не чекаючи потенційних багаторазових повторних передач ненадійною або втраченою ланкою 1-2, можна замінити відправлення пакетів на ланки 3-5 або 4-6,і, таким чином, передати пакет в приймальний вузол 7. Якщо щонайменше одна ланка буде здатна доставити пакет успішно, пакет може бути прийнятий і далі прямуватиме до місця призначення.

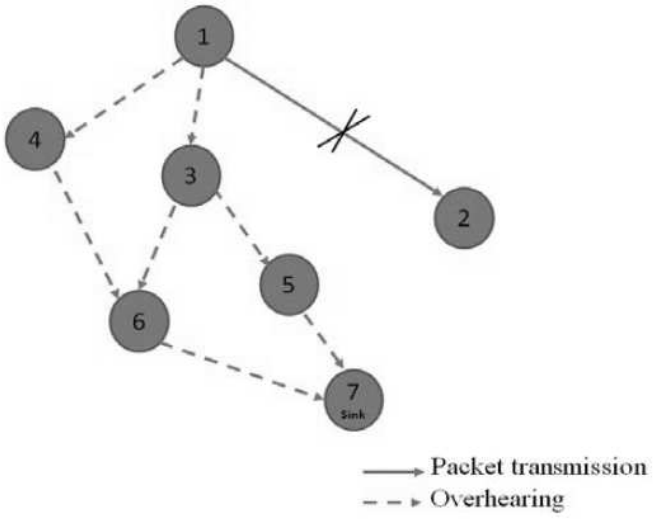


Рис. 1 Схема ретрансляції з використанням «співпраці» вузлів

Це стало можливим завдяки координації дій між вузлами, що мають місце шляхом обміну керуючими повідомленнями. Ймовірність виходу з ладу однієї ланки більша, ніж всіх ланок разом. Таким чином, альтернативні відповідні з'єднання можуть підвищити надійність мережі, а також зменшити затримку при передачі пакету заново від початкового вузла до останнього. Економія енергії для уникнення повторних передач за втраченим з'єднанням може компенсувати енергію, що споживається на «підслухування» пакетів. Співпраця між вузлами знижує споживання енергії при одночасному досягненні надійності.

При використанні протоколу вузли повинні домовитися про те, які з їхньої підмножини вузли матимуть право ретранслювати втрачений пакет, і

за яких обставин повторна передача повинна матиме місце. Метрика, що відображає вартість надійності кожного з'єднання, має бути відомою для класифікації вузлів і для визначення найкращого вузла для перенесення повторно переданого сигналу.

Індекс сусіднього вузла використовується для класифікації вузлів залежно від їх важливості. Призначення індексу сусідньому вузлу базується на метриці, що відображає якість з'єднання. Більш надійним є з'єднання з нижчим індексом. Тому вузол з індексом 0 має найкращу метрику. Також протокол забезпечує унікальність індексів, щоб уникнути проблем колізії. Кожен вузол знає свій індекс по відношенню до вузла, що знаходиться вище.

Після того, як пакет з ідентифікатором пакету (PID) приймається перший раз вузлом рангу N від вузла рангу N + 1, пакет зберігається, і пов'язаний з ним перехідний контекст створюється в пам'яті для управління цим пакетом PID. Кожен вузол пов'язує перехідний контекст для кожної пари, а саме: ідентифікатор пакету вузла відправника і вузла отримувача. Розрізняють два типи: первинний і вторинний контекст. Первинний контекст пов'язаний з вузлом з найкращою метрикою (рівень 0 на початку) щодо вузла відправника. В іншому випадку, контекст розглядається як вторинний. Для вузла з первинним контекстом пакет даних буде негайно відправлений, в той час як для вузла з вторинним контекстом пакет буде поміщено в буфер прийнятих пакетів і чекатиме можливого запиту на повторну передачу. Контекст може бути модернізований з первинного до вторинного.

Література

1. A.E.Khandani, J.Abounadi, E. Modiano, and L.Zheng. Cooperative Routing in Static Wireless Networks. IEEE TRANSACTIONS ON COMMUNICATIONS, pages 2837-2842, 2007.
2. G. Li, Z. Xu, C. Xiong, C. Yang, S. Zhang, Y. Chen, and S. Shugong Xu. Energy efficient wireless communications: tutorial, survey, and openissues. IEEE Wireless Communications, pages 28-35, 2011.
3. M. A. Mahmood and W. Seah. Reliability in Wireless Sensor Networks: Survey and Challenges Ahead. Preprint submitted to Elsevier, pages 1-42, 2012.

UDC 519.85

THE SYSTEM OF INJECTION OF SUBMINIATURE SATELLITES (NANOSATELLITES) TO NEAR-EARTH ORBIT ON THE BASIS OF AH-124-100 AIRPLANE

Tachinina O.
National Aviation University, Ukraine
E-mail:tachinina@rambler.ru
Chekanova I., Lysenko O., Alekseeva I.
National Technical University of Ukraine "KPI", Ukraine
E-mail: lysenko.a.i.1952@gmail.com
Chumachenko S.
Ukrainian Scientific Research Institute of Civil Protection, Ukraine
E-mail: s_chum@ukr.net

СИСТЕМА ВЫВЕДЕНИЯ СВЕРХМАЛЫХ СПУТНИКОВ (НАНОСПУТНИКОВ) НА ОКОЛОЗЕМНУЮ ОРБИТУ НА БАЗЕ САМОЛЕТА АН-124-100

В статье предложен способ выведения наноспутников на околоземную орбиту на базе самолета Ан-121-100, позволяющий снизить стоимость запуска и увеличить доступность данного способа в сравнении с «классическими» ракетами-носителями для выведения спутников.

Beginning of the third millennium coincided with a new stage of development of technologies of miniature spacecraft: micro- and nano-satellites. Nano-satellites (nanosatellites, nanosats) are spacecraft with a mass from 1 kg to 10 kg, the size of 1U (10*10*10 cm), 2U (10*10*20 cm) and 3U (10*10*30 cm), designed to solve simple and important tasks. Nanosatellites will be used for remote sensing, environmental monitoring, earthquake prediction and study of the ionosphere.

The time of individual breakthroughs and first successful experiences of small satellites building is over. The main task today is the insertion of nanosatellites into orbit. The cluster launches of subminiature satellites on large launch vehicles have inherent disadvantages.

It is proposed to launch nanosatellites as a payload on the basis of An-124-100 airplane, which is used as a mobile launch pad to launch the SS-24 light class solid-propellant launch vehicle (LV). The airplane with LV placed in cargo compartment will take off from a conventional airfield and lift to a height of about 20 km, where with the help of air-launcher including transporter-erector-launcher (TEL) and parachute system.

The LV located on the TEL starts to move on the floor equipment (rollers) under the parachute forces towards the cargo door as a result of preparations for the dropping operations related to cargo door opening, activation of control systems, etc. The belts binding the LV and TEL or other devices are disconnected at the moment of physical separation from the airplane.

Using own solid-propellant engine (during the initial stage of the flight) and from force of inertia afterwards the LV with the launch container including nanosatellites, goes to a height of about 600 km which is targeted for dropping a payload in the form of miniature satellites. Following this the TEL lands by means of parachute in a

predetermined position and is ready for further (multiple) use. The nanosatellites are installed on the platform inside the container and are pressed to the cover by springs.

The electric pulse from the LV activates the release mechanism of the cover that rotates 170° and a nanosatellite is separated along the guide rails by spring mechanism to predetermined speed, which is determined by the used spring and nanosatellite weight. A small payload is separated due to the magnetic-impulse drive with capacitive energy storage.

The proposed project is best suited to existing and other potential limitations owing to launching from airplane using customers' aerodromes and air space.

Fundamentals of business. The injection of subminiature satellites (nanosatellites) into near-earth orbit on the basis of An-124-100 airplane:

- allows to reduce significantly the launch cost and increase the availability of this method in comparison with the classic satellite launch vehicles;
- simplifies the preparation of nanosatellites launch (the customer waits for vacancy in launch vehicles from a few months to several years when the conventional launch vehicles are used);
- induces mass use of general-purpose small satellite due to low cost of launch.

The project involves the wide use of existing practices and technology.

Existing markets of launching. Market of launches is a relatively new and dynamic sector of the world market of high-technology services. Ukraine controls almost 10% of the international launch market. Euroconsult research company (Paris) expects that the market of space launches will increase significantly next 10 years. The experts note that the expansion of space capabilities of developing countries, in particular India and China, will favor to reduce the price of the spacecraft production services, thereby increasing the demand for launch services for the injection of nanosatellites into near-earth orbit.

Target customer profile. The target customers interested in existing practices and techniques for injection of subminiature satellites (nanosatellites) into near-earth orbit are: Ministries and Departments as well private and public corporations-manufacturers of satellites up to 10 kg, institutes from all over the world, research laboratories and various centers, who need to inject small size spacecraft into near-earth orbit to continue research, experiments and remote sensing the Earth, environmental monitoring, earthquake prediction, ionosphere study, nonterrestrial objects and space study, human possibilities expansion and access to space for millions of worldwide people.

In addition, large groups of nanosatellites in the future will enable to solve complex tasks requiring more accurate and quality data about our planet and space around.

A new advanced application is usage of nanosatellites as a platform for nanotechnology experiments, nano-components and materials testing. Nanosatellites with small size and weight are simple and cheap means of scientific research in the short-range space.

Sizes and rate of growth of the target markets. The market size is determined by number of customers.All existing (and future) launch vehicles are evaluated according to a common criterion of efficiency – by cost for orbital injection of one kilogram of payload. Nowadays the unit cost of injection into orbit varies from 10,000 to 20,000 $

per one kg of payload. This is a major constraint for further development (extension) of the market. According to some estimates, the market of nanosatellites injection into orbit could reach $ 2.5 billion by 2018.

Currently nanosatellites injections into orbit are carried by conventional launch vehicles. PolyITAN-1 nanosatellite (Ukraine, about 1 kg in weight and 10*10*10 cm by size), created in Kiev Polytechnic Institute, was injected into near-earth orbit by Dnepr launch vehicle (Ukraine) with the aid of the launching containers with 33 nano-satellites, created by scientists from 17 countries. The launch was made from Yasniy launch facility at 23:11 local time, June 19, 2015. There are no competitors in the market of Ukraine for nanosatellites injection into orbit on the basis of An-124-100 airplane.

The indirect competitors to launch nanosatellites into orbit are Celestia Aerospace company (Spain, it intends to get to nano-satellites market by development, production and launch of nano-satellites on demand), companies from the United States and Russia (SoyuzStart-H centre of nanosatellites launch services). The nano-satellites are injected by means of launch vehicles requiring a lot of time and costs.

Strategy. In order to gain a foothold in the world market the basis of the strategy should be consistent position to increase investment in new quality production.

To promote the product to the world markets both regional and the concentrated sharing space technology markets, the formation and use of the new global business strategies, various and multifaceted marketing strategies are characteristic features.

It is supposed to use the innovative marketing strategies, to study in-depth types and forms of the world market, its operation environment, to analyze recent research and publications, dynamics of development and functioning of the world's space launches, to study scientific and technological level of design, trends of global competitiveness transforming.

In order to expand successfully our participation in international cooperation and world space projects, as well to increase in future the share of Ukraine space products at the world market, it is necessary also to investigate the basic factors, trends and characteristics that affect the criteria of formation and relationship of functioning of launch markets.

The proposed method of nanosatellites launching into orbit on the basis of AN-124-100 airplane is planned to implement by government customers interested in using the existing developments with subsequent entering to the world space market.

Rererences

1. Belokonov I., Skobelev P., Zhilyaev A.A., Multi-agent planning of the network traffic between nanosatellites and ground stations // The 65th International Astronautical Congress. IAC-2014, Toronto, P. 7113-7123.
2. Schaub H., Junkins J. Analytical mechanics of space systems. 2nd ed. AIAA, 2003. P. 794.

УДК 621.3

МЕТОД ВИКОРИСТАННЯ ГЕОМЕТРИЧНИХ ФРАКТАЛІВ ДЛЯ РОЗВ'ЯЗАННЯ ЗАДАЧІ ОПТИМАЛЬНОГО РОЗМІЩЕННЯ СЕНСОРІВ ПРИ ЕКОЛОГІЧНОМУ МОНІТОРИНГУ

Томашевська Т.В., Гордійко Н.О., Прищепа Т.О., Лисенко О.І.
Національна Академія статистики, обліку та аудиту
tomas_tat@ukr.net
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
prischepa@i.ua, Lysenko.a.i.1952@gmail.com

Method of using geometrical fractals for solving problems optimal sensor placement of environmental monitoring

This article describes the method of solving the problem of optimal placement of system sensors in environmental monitoring. The proposed location of the sensors in the centers or intersections of the "cells" of a geometric fractal object, the shape of which corresponds to the geometry of the field observation was chosen as the template host. Given the result of the calculation for the monitoring of arbitrary shape.

Вирішення кардинальних проблем у екологічній політиці держави тісно пов’язане із здійсненням низки завдань з охорони довкілля. Серед них важливе місце займає створення служби моніторингу, яка на основі зібраних даних дає рекомендації щодо техногенної безпеки навколишнього середовища та розробки раціональних способів його використання. Моніторинг має три ступеня: спостереження, оцінка стану і прогноз можливих змін. Він здійснюється, передусім, за антропогенними змінами, адже в сучасну епоху, власне, вплив людини на природне середовище спричинює небезпечні зміни природних комплексів.

Первинний етап моніторингу полягає у спостереженні за станом довкілля, зокрема, за допомогою відповідної системи датчиків, що створюють "фотографію" екологічного стану об’єктів моніторингу.

Для більшості антропогенних факторів характерним є імпульсно-точковий характер, що потребує раціонального охоплення датчиками всієї інспектованої території.

В той же час екологічні дані носять досить громіздкий характер і належать до категорії надмірних, тому однією з задач є обмеження обсягів даних ще на першому етапі моніторингу – спостереженні за рахунок оптимізації їх кількості.

Розрахувати кількість датчиків, необхідну для покриття всієї області спостереження дуже просто, знаючи радіус їх дії та площу території. Проте

потрібно раціонально їх розмістити: щоб не було ані неохоплених ділянок (що призведе до браку інформації), ані перекриття (надлишок інформації).

Отже, проблема оптимального розташування датчиків при екологічному моніторингу є досить актуальною.

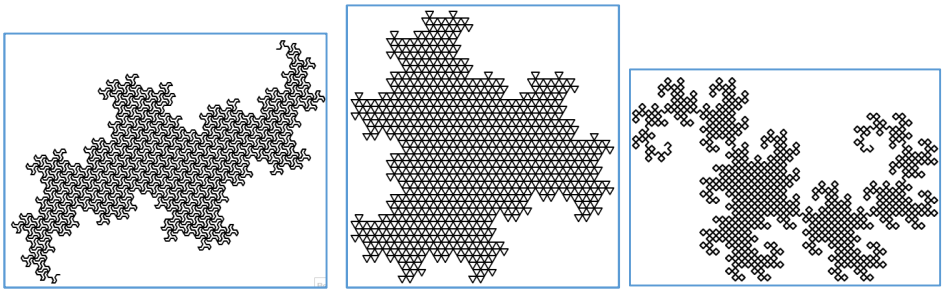
Як відомо [1,3], фрактальні криві, зокрема, геометричні, досить оптимально розміщуються на обмеженій області певної форми, оскільки їх можна віднести до множини всюди щільних кривих. Виходячи з цього, для вирішення поставленої проблеми пропонується проаналізувати геометрію області спостереження, підібрати такий геометричний фрактальний об'єкт, що відповідатиме їй (оптимальним чином розміститься на ній) та розташувати в його "комірках" (або на їх перетині) датчики системи екологічного моніторингу, тобто використати його як шаблон. Таким чином можна охопити датчиками територію спостереження, не обтяжуючи систему їх кількістю, тим самим не перевантажуючи інформаційну систему екологічного моніторингу.

Постановка задачі. Метою роботи є створення на базі геометричних фрактальних об'єктів методу розв'язання задачі оптимального розташування системи датчиків для використання в системах екологічного моніторингу. Побудований фрактальний об'єкт стане шаблоном розміщення датчиків.

Використання принципів теорії фракталів при екологічному моніторингу виходить з самого характеру фрактальних об'єктів [2], дозволяє зменшити розкидане хаотичне розростання кількості датчиків і тим самим оптимізувати систему екологічного моніторингу.

У роботі розглядається найбільш наочний клас фрактальних об'єктів – геометричні фрактали. Для побудови об'єктів цього типу використовуються L-системи та терл-графіка [4], за допомогою яких можна створювати нескінченне різноманіття фракталів.

Звичайно, для областей правильної форми не має сенсу використовувати фрактали. Проте реальні форми територій моніторингу не є простими. А серед різноманіття фрактальних об’єктів можна відшукати відповідний шаблон неправильної форми, наприклад: Tiling1 (рис.1,а), Triangle (рис.1,б), дракон Хартера-Хейтуея (рис.1,в) тощо.



а) б) в)

Рис. 1. Приклади фрактальних об’єктів неправильної форми.

Використовуючи фрактальний об'єкт як шаблон для розміщення датчиків спостереження системи екологічного моніторингу, можна її оптимізувати. Зважаючи на геометрію області спостереження, можна розмістити інформаційні датчики у центрах або на перетинах "комірок" фрактального об'єкту таким чином, щоб вся територія спостереження охоплювалась датчиками і, водночас, не була надмірною. Це дасть можливість оптимізувати систему моніторингу щодо кількості датчиків та тим самим оптимізувати кількість корисної інформації, отриманої за їх допомогою.

На прикладі області спостереження довільної форми показано застосування запропонованого методу з використанням фрактального об’єкту Triangle.

Перспективи подальшого розвитку полягають у застосуванні запропонованого методу оптимального розміщення у різних системах моніторингу. Зокрема, в останні роки актуальним стає обстеження щодо виявлення шкідливих речовин територій військових полігонів, які, на жаль, стали використовуватися частіше. Забруднюючі речовини, що з'явилися на полігоні в результаті його функціонування, можуть потрапляти у повітря, а також у наземні та підземні водойми, річки, артезіанські свердловини тощо. Тому потрібні постійні заходи контролю. Форма обстежуваної території, як правило, не має простої геометричної форми. Тому, використовуючи властивості фракталів, можна шляхом створення нових фрактальних об'єктів (змінюючи породжуючі правила), максимально наблизити форму фрактального об'єкту до форми області спостереження та автоматизувати процес екологічного моніторингу, створивши, наприклад, інформаційно-довідкову систему шаблонів.

Література

1. Мандельброт, Б. Фрактальная геометрия природы / Б. Мандельброт; [пер. с англ. А. Р. Логунова]. – М. : Институт компьютерных исследований, 2002. – 656 с.
2. Фракталы и мультифракталы в биоэкологии : монография / [Д. Б. Гелашвили, Д. И. Иудин, Г. С. Розенберг, В. Н. Якимов и др.]. – Нижний Новгород: Изд-во Нижегородского госуниверситета, 2013. – 370 с.
3. Федер, Е. Фракталы / Е. Федер; [пер. с англ. Ю. А. Данилова, А. Шукурова] – М.: Мир, 1991. – 254 с.
4. Кроновер, Р.М. Фракталы и хаос в динамических системах. Основы теории / Р. М. Кроновер. – М.: Постмаркет, 2000. – 352 с.

УДК 621.396

ШВИДКА ОПТИМІЗАЦІЯ ЛІПШИЦА У БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ

Трач Б.В., Лисенко О.І.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: bv.trach@gmail.com

Fast Lipschitz Optimization in Wireless Sensor Networks

Fast Lipschitz Optimization method is considered. It allows efficiently solving optimization tasks in distributed systems, for example in wireless sensor networks. Its performance indicators have better convergence properties than typical Lagrangian methods. Such algorithms are potentially applicable for distributed target detection and radio transmitter power control.

На даний момент безпроводові сенсорні мережі є важливим інструментом дослідження фізичного світу. Їх важливість пов'язана з новими можливостями використання, що обумовлені такими характеристиками БСМ, як відсутність необхідності у кабельній інфраструктурі, мініатюрність вузлів, низьке споживання електроенергії, вбудований радіоінтерфейс, досить висока обчислювальна здатність, порівняно невелика вартість. Все це зробило можливим їх широке застосування у багатьох сферах людської діяльності з метою автоматизації процесів збору інформації, моніторингу, контролю характеристик різноманітних технічних та природніх об'єктів [1]. При цьому у зв’язку з обмеженими ресурсами окремих вузлів для вирішення багатьох задач необхідна кооперативна робота всіх вузлів мережі для досягнення цілі.

При цьому багато задач, що виконуються безпроводовими сенсорними мережами, зводяться до розподіленого вирішення задач оптимізації, у яких кожен вузол підстроює свої параметри з урахуванням інформації на сусідніх вузлах. Для виконання такої задачі розроблена велика кількість методів [2], однак вони не були спеціально розроблені для використання в безпроводових сенсорних мережах. Як наслідок цього при їх застосуванні виконується надлишковий обмін даними, якого можна було б уникнути при застосуванні більш досконалих алгоритмів. Одним з таких алгоритмів є алгоритм швидкої оптимізації Ліпшица [3], що полягає у використанні властивостей стискаючих відображень Ліпшица, і дозволяє одержати сходження до оптимального результату швидше, ніж при використанні методів Лагранжа.

Мета дослідження — дослідження алгоритмів розподіленої мережевої оптимізації. Об'єктом дослідження є алгоритм швидкої оптимізації Ліпшица. Предметом дослідження є розподілена локалізація вузлів у безпроводових сенсорних мережах.

Розглянемо задачу оптимізації у її загальній форм. Нехай необхідно знайти максимум функції:

$$\max_{x} f_0(\boldsymbol{x}) \qquad (1)$$

за певних обмежень-нерівностей та обмежень-нерівностей:

$$x_i \le f_i(\boldsymbol{x}), i = 1,\ldots,l \tag{2.1}$$

$$x_i = h_i(\boldsymbol{x}), i = l+1,\ldots,n \tag{2.2}$$

$$\boldsymbol{x} \in D, \tag{2.3}$$

де D — не порожня, випукла, компактна множина, $l \le n$, а цільова функція та обмеження неперервні диференційовані функції, такі що

$$f_0(\boldsymbol{x}) : D \to R^m, \quad m \ge 1 \tag{3.1}$$

$$f_i(\boldsymbol{x}) : D \to R, i = 1,\ldots,l \tag{3.2}$$

$$h_i(\boldsymbol{x}) : D \to R, i = l+1,\ldots,n \tag{3.3}$$

Розглянемо умови, за яких до задачі можна застосувати метод швидкої оптимізації Ліпшица. Нехай

$$\mathbf{f}(\boldsymbol{x}) = [\, f_1(\boldsymbol{x}),\, f_2(\boldsymbol{x}),\ldots,\, f_l(\boldsymbol{x})]^T \tag{4.1}$$

$$\mathbf{h}(\boldsymbol{x}) = [h_{l+1}(\boldsymbol{x}),\, f_{l+2}(\boldsymbol{x}),\ldots,\, f_n(\boldsymbol{x})]^T \tag{4.2}$$

$$\mathbf{F}(\boldsymbol{x}) = [F_i(\boldsymbol{x})] = [\mathbf{f}(\boldsymbol{x})^T, \mathbf{h}(\boldsymbol{x})^T]^T \tag{4.3}$$

Тоді необхідно перевірити виконання наступних умов:

$$\nabla f_0(x) \succ 0,\ f_0(x) \text{ строго зростаюча.} \tag{5.1а}$$

$$\|\nabla \mathbf{F}(\boldsymbol{x})\| < 1 \tag{5.1б}$$

і або:

$$\nabla_j F_i(\boldsymbol{x}) \ge 0, \forall i, j \tag{5.2}$$

або:

$$\nabla_i f_0(\boldsymbol{x}) = \nabla_j f_0(\boldsymbol{x}), \tag{5.3а}$$

$$\nabla_j F_i(\boldsymbol{x}) \le 0, \forall i, j \tag{5.3б}$$

$$\|\nabla \mathbf{F}(\boldsymbol{x})\|_\infty < 1, \tag{5.3в}$$

або:

$$f_0(\boldsymbol{x}) \in R, \tag{5.4а}$$

$$\|\nabla \mathbf{F}(\boldsymbol{x})\| \le \frac{\beta}{\beta + \Delta}, \tag{5.4б}$$

де $\beta = \min\limits_{i, x \in D} \nabla_i f_0(\boldsymbol{x}),$

$\Delta = \max\limits_{i, x \in D} \nabla_i f_0(\boldsymbol{x}).$

За таких умов задача оптимізації допускає вирішення швидким методом Ліпшица. Крім того, формули (5.1-5.4) можливо подати і у іншому вигляді [4]. Вибір умов для перевірок слід вибирати залежно від вигляду обмежень-рівностей та обмежень-нерівностей.

Знаходження оптимального значення використовується наступна

властивість сходимості: нехай $\boldsymbol{x}(0) \in D$ початкова оцінка оптимального рішення, а $\boldsymbol{x}^i(k) = [x_1(\tau_1^i(k)), x_2(\tau_2^i(k)), \ldots, x_n(\tau_n^i(k))]$ — вектор змінних на вузлі i в момент часу $k \in N$, де $\tau_i^j(k)$ — затримка з якою змінна вузла j досягає вузла i. У цьому випадку наступний алгоритм сходиться до оптимального рішення:

$$\begin{aligned} x_i(k+1) &= [f_i(\boldsymbol{x}^i(k))]^D, i = 1, \ldots, l \\ x_i(k+1) &= [h_i(\boldsymbol{x}^i(k))]^D, i = l+1, \ldots, n \end{aligned} \tag{6}$$

де $k \in N_+$ — цілочисельний номер ітерації.

Згідно з цією властивістю кожен вузол мережі оновлює свої змінні за ітеративним алгоритмом (6) та з використанням тих змінних інших вузлів, що наявні у нього на час ітерації. Слід зазначити, що якщо $f_i(\boldsymbol{x})$ залежить лише від змінних сусідніх вузлів, обмін цими даними може виконуватись з високою ефективністю. У деяких задачах, наприклад оптимізації енергоспоживання, можна використовувати цей алгоритм без обміну інформації [5].

На практиці буває корисно знати максимальну кількість ітерації алгоритму, яку необхідно виконати для сходження алгоритму до заданої точності η. Нехай

$$d = \max_{x, y \in D} \| \boldsymbol{x} - \boldsymbol{y} \|_\infty \tag{7}$$

Тоді при $\eta < d$ для знаходження розв'язку з заданою точністю необхідна кількість ітерації, що пропорційна $\bar{k}$,

$$\bar{k} = \frac{|\ln \eta| - |\ln d|}{|\ln \alpha|} \tag{8}$$

де α константа Ліпшица для $\mathbf{F}(\boldsymbol{x})$ при $x \in D$:

$$\alpha = \max_x \| \nabla F_i(\boldsymbol{x}) \| < 1, \forall i = 1, \ldots, n. \tag{9}$$

Таким чином у роботі описано алгоритм швидкої оптимізації Ліпшица, надано умови його застосування до задач оптимізації, та нерівність для визначення необхідної кількості ітерацій. Ці методи можуть застосовуватись для вирішення задач, що виникають у безпроводових сенсорних мережах у широкому ряді практичних задач.

Література

1. Ian F. Akyildiz, Weilian Su, Yogesh Sankaraubramaniam, and Erdal Cayirci: A Survey on sensor networks, IEEE Communications Magazine (2002).
2. Dimitri P. Bertsekas and John N. Tsitsiklis: Parallel and Distributed Computation: Numerical Methods (2015), 735 pages.
3. Carlo Fischione, Fast-Lipschitz optimization with wireless sensor networks applications, 10th International Conference on Information Processing in Sensor Networks (IPSN) (2011), pages: 378 – 389.
4. Martin Jakobsson, Carlo Fischione, Pradeep Chathuranga Weeraddana: Extensions of Fast-Lipschitz Optimization, (2014) Онлайн-ресурс http://arxiv.org/abs/1309.0462 (останній доступ 29.02.2016).
5. M. Schubert and H. Boche, QoS-Based Resource Allocation and Transceiver Optimzation, Foundations and Trends in Communications and Information Theory. Boston, MA: NOW, 2005.

УДК 621.396

СПОСОБИ ПІДВИЩЕННЯ НАДІЙНОСТІ БЕЗПРОВІДНИХ СЕНСОРНИХ МЕРЕЖ

Туранська О.С., Прищепа Т.О.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: tos.kpi@gmail.com

Ways to Improve Reliability of Wireless Sensor Networks

This work examines mathematical models for the estimation of reliability of wireless sensor networks and their classification. Features of wireless sensor networks are brought, touch-control architecture, the value of sensory networks in different industries and in our life is also considered.

На сьогоднішній день використання безпровідних сенсорних мереж (БСМ) є перспективною і невід'ємною частиною розвитку сучасних телекомунікацій та вирішення завдань широкого кола значень. Основними особливостями БСМ є самоорганізація і адаптивність до змін в умовах експлуатації, тому потрібні мінімальні витрати при розгортанні мережі на об'єкті і при подальшому її супроводі в процесі експлуатації. Саме це приваблює користувачів БСМ, яких стає все більше з кожним днем. Тому постійно виникає необхідність покращення характеристик БСМ, однією з яких є надійність.

Головною перевагою систем на основі сенсорних мереж є надійність мережі в цілому – в разі виходу з ладу одного з вузлів інформація передається через сусідні елементи.

Найбільш суттєвими факторами, що впливають на надійність мережі є: надійність апаратного та програмного забезпечення вузлів, область розгортання мережі, взаємне розташування вузлів, період регламентного обслуговування мережі, інтенсивність збору та передачі інформації кінцевими вузлами (вузли, оснащені сенсорами і здійснюють вимірювання), розмір переданих пакетів інформації.

WSN складається з великої кількість вузлів-датчиків, що розгорнуті на певній території і надають дані в реальному часі про певні явища. Основними областями застосування БСМ (WSN)виступають: військові операцій, зонні спостереження, охорона навколишнього середовища і довкілля, моніторинг, дистанційне зондування та глобальна поінформованість. Розгортання WSN може бути виконано випадковим чином (опускаючи датчики у ворожу місцевість або зону лиха) або детермінованим(розміщення датчиків уздовж трубопроводу для моніторингу тиску і/або температури). Проте, в обох випадках потрібно налаштувати WSN з максимальною надійністю кластерів. Кожен кластер має одну або кілька касетних головки. Вони прикріплені на вузол, який може бути базовою станцією або кінцевим користувачем, як

правило, за допомогою декількох шлюзів або ретрансляційних вузлів. Це необхідно для забезпечення високої надійності, відмовостійкості кластерів з великою кількістю дешевих датчиків і використання надмірності разом з методами інформаційної інтеграції (агрегації) і синхронізації.

Два основні чинники впливають на ймовірність відмови датчика вузла: по-перше, це обмежені ресурси і низька вартість виробництва, по-друге, різкий характер середовища WSN додатків. Надійний моніторинг (або виявлення подій) залежить від колективних даних, наданих цільовим кластером датчиків, а не з кожного окремого вузла.

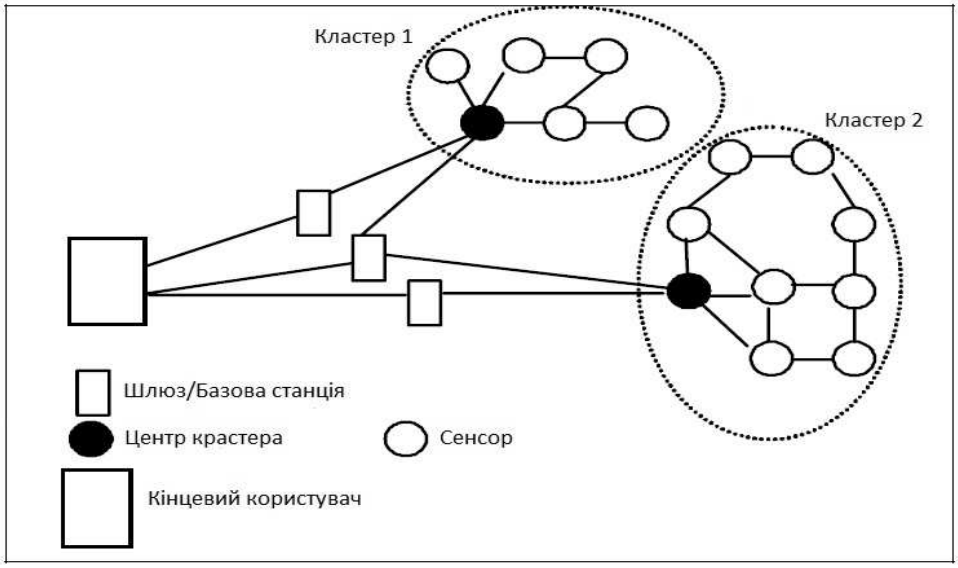


Рис. 1 Структура БСМ. Кластери, шлюзи та сенсорні вузли.

Для оцінки надійності безпровідних сенсорних мереж існує декілька математичних моделей. Підхід до оцінювання надійності базується на представленні функціонування безпровідної сенсорної мережі як марківського процесу і припускає використання математичної моделі надійності передачі даних між двома вузлами такої мережі, яка, в свою чергу, являє собою композицію моделей надійності вузлів, комунікацій між ними та механізму їх доступу до середовища.

Існують наступні математичні моделі підвищення надійності: модель надійності передачі пакетів між двома вузлами, модель надійності вузла, модель надійності комунікацій між вузлами, модель впливу ефекту прихованого вузла

Модель надійності передачі пакетів між двома вузлами описується виразом, що визначає ймовірність успішної передачі пакета від одного вузла іншому. Алгоритм розрахунку даної ймовірності заснований на одному з можливих принципів роботи механізму маршрутизації. На кожному вузлі є обмежена таблиця маршрутизації, записи в якій ранжовані по перевагах

використання кожного напрямку передачі. Ємність таблиці маршрутизації може бути обрана довільно при побудові мережі.

Обмеження на надійність вузлів безпровідної сенсорної мережі обумовлена розрядом батареї в процесі роботи мережі, а також можливістю виходу їх з ладу, викликаного різними факторами: відмовою апаратного та програмного забезпечення, зовнішніми впливами та ін.. Необхідно врахувати, що основне споживання енергії вузлом відбувається при активній роботі його приймача або передавача, тому час розряду батареї буде обернено пропорційний довжині пакетів і сукупної інтенсивності їх прийому/передачі. Заміна розряджених батарей здійснюється періодично та одночасно для всіх вузлів. Дана модель носить назву «модель надійності вузла».

У зв'язку з особливостями експлуатації БСМ має місце модель надійності комунікацій між вузлами. Втрата пакетів також може відбуватися через наявність шумів, що в свою чергу може вплинути на надійність мережі. У даній моделі ймовірність успішної передачі повідомлення залежить від довжини самого повідомлення та ймовірності безпомилкового прийому символу даних.
Модель впливу ефекту прихованого вузла описує розподілені безпровідні мережі, які не володіють повною зв'язністю. В процесі передачі пакету *i*–им вузлом на адресу *j* -го вузла може також відбуватися передача пакета вузлом, що знаходяться в радіусі досяжності *j*-го, але за межами радіуса досяжності *i*-го вузла, що призводить до колізій на *j*-му вузлі. Це викликає затримку передачі, що знижує ймовірність успішної доставки пакета. Цей вплив на надійність БСМ посилюється при збільшенні мережевого трафіку.

В ході роботи над даною темою було розглянуто особливості архітектури сучасних безпровідних сенсорних мереж та їх характеристика, які визначають їх переваги перед іншими рішеннями в галузі моніторингу: автономність вузлів, можливість розміщення у важкодоступних місцях, мале енергоспоживання, здатність до самоорганізації. Також розглянуто можливі методи підвищення надійності БСМ та їх математичні моделі.

Література

1. Акимов Е.В., Кузнецов М.Н. Вероятностные математические модели для оценки надежности беспроводных сенсорных сетей // Электронный журнал «Труды МАИ». Выпуск № 40// URL: http://www.mai.ru/science/trudy/
2. Hossam. M. F. Abo El Fotoh, Ehab. S. El Mallah, Hossam. S. Hassanein**.** On The Reliabilityof Wireless Sensor Networks // INTERNATIONAL JOURNAL OF SENSOR NETWORKS 2(5/6):311-320 · JANUARY 2007 *with* 39 READS//URL :https://www.researchgate.net.
3. Половко А.М., Гуров С. В. Основы теории надежности. – СПб.: БХВ-Петербург 2006. – 560 с.

УДК 621.39

ПІДХОДИ РЕАГУВАННЯ НА НАДЗВИЧАЙНІ СИТУАЦІЇ ІЗ ЗАСТОСУВАННЯМ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ

Хоменко Є.О., Валуйський С.В.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: katyn.katun@gmail.com

Approaches for emergency response using wireless sensor networks

The use of wireless sensor networks for indoor navigation in emergencies and approaches for emergency response are considered. Direction of further development these approaches is investigated.

Бездротові сенсорні мережі відіграють важливу роль у виявленні надзвичайних ситуацій і навігації людей з небезпечних районів [1]. У цій роботі розглядаються недавні дослідження з використанням сенсорних мереж і комп'ютерних систем для підвищення безпеки людей в надзвичайних ситуаціях. Робота в основному фокусується на пошуку шляху (алгоритми для забезпечення безпечної евакуації) та прийняття рішень системою[2].

Моніторинг в реальному часі і швидке реагування є невід'ємними вимогами, що містяться в конструкції системи екстреного реагування [3-4].

Існує два типи підходів до ліквідації надзвичайних ситуацій, (підхід 1 і підхід 2 на рис. 1) [5]. Перший підхід ґрунтується на фіксованих бездротових сенсорних мережах (БСМ). При цьому взаємозв’язок між тими, хто евакуюються і системою надзвичайних ситуацій, відбувається за допомогою електронних дисплеїв-«провідників». Сама ж система повинна динамічно приймати рішення. Підхід 2 фокусується на використанні мобільних пристроїв, а також датчиків, так що жертви надзвичайної ситуацій та персонал може діяти автономно на основі рекомендацій та інформації, яку вони отримують кожен особисто на свої мобільні пристрої.

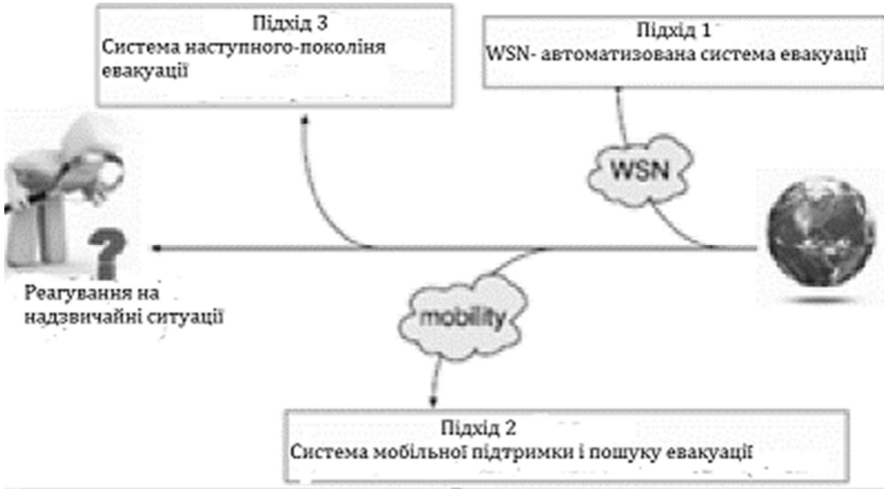


Рис.1. Система для реагування на аварійну ситуацію.

Пошук безпечних шляхів евакуації і представлення її своєчасно до тих, що евакуюються є основним завданням динамічних систем надзвичайних ситуацій[6].

Тому ми розглянемо три класи розподілених протоколів для обчислення безпечних шляхів евакуації.

- *Підхід потенційно-технічного обслуговування [7]*.

Кожен користувач оснащений сенсорним вузлом для зв'язку з WSN, який дозволяє запросити шлях невідкладної евакуації. Передбачається, що WSN повинен бути відомий кожному користувачеві. Таким чином мета методу полягає в тому, щоб знайти " безпечний " шлях від кожного датчика до виходу, минаючи будь-які перешкоди. Концепція штучних потенційних полів, які вже давно використовуються для розрахунку шляхів евакуації в розподілений спосіб: датчик виходу створює привабливий потенціал, щоб «тягнути» датчики до виходу, в той час як кожна перешкода створює відштовхуючий потенціал, щоб «відштовхнути» датчики від перешкоди. Таким чином, кожен датчик може обчислити загальне потенційне значення, що використовується для направлення евакуйованих. При цьому загальна потенційна величина датчиків обчислюється:

$$P(S_i) = \sum_{S_h \in H} \frac{1}{d^2(s_i, s_h)}, \quad (1)$$

де H – безліч датчиків, які виявляють перешкоди, і d (s_i, s_h) – найкоротша відстань до перешкоди.

- *Геометричні підходи [7]*.

Такі підходи використовують унікальні властивості геометричних графів для планування шляхів евакуації якнайдалі від небезпек, наскільки це можливо. Наприклад, WSN поділяють на кілька трикутних областей для планування площі шляху навігації, як показано на рис. 2; кожен датчик знає своє місце розташування і буде співпрацювати, щоб обчислити плоский граф. Небезпеки будуть трьох кольорів на підставі показників датчиків (для відображення різного ступеню небезпеки). Червоний колір використовується, якщо всі три датчики бачать небезпеку. Зона забарвлена жовтим кольором, якщо два датчика на вихідному краю виявили небезпеку, але залишився ще один в «безпеці». В іншому випадку, зона має зелений колір. Навігаційний напрямок кожної трикутної зони перераховується, щоб гарантувати безпеку для тих що евакуюються.

- *Підхід на основі прогнозування [7]*.

У той час як більша частина досліджень зосереджена на пошуку шляхів на основі інформації в реальному часі, даний підхід використовує пророкування того, як довго небезпеці потрібно, щоб досягти датчика, для обчислення шляху евакуації з найдовшим шляхом. Безпечні шляхи евакуації, в даному методі розраховуються за допомогою «графу небезпеки» і «графу навігації». Кожен датчик має відповідну вершину в обох графах. І найбезпечніший шлях вираховується як найсприятливіше відношення даних цих графів, тобто мінімальний шлях до найнебезпечнішої перешкоди.

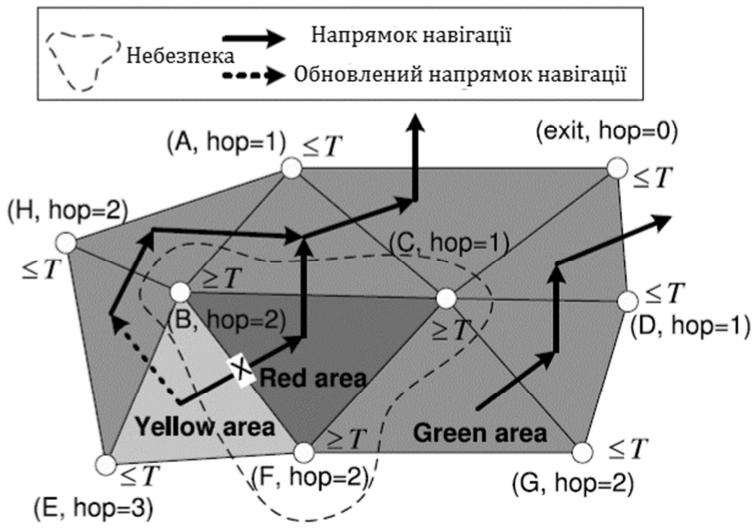


Рис.2. Приклад площі області навігаційних шляхів

Третій підхід до ліквідації надзвичайних ситуацій буде фокусуватися на технологіях нового покоління, як спосіб проведення передбачення поширення небезпек, під час надзвичайної ситуації з переміщенням об'єктів, таких як роботизовані ресурси і людина. Така модель також зможе враховувати середню поведінку людей і заздалегідь реагувати на «непередбачувану поведінку» людей. Імовірнісні моделі також можуть бути використані для оцінки ризику і збитку, а також для моделювання ефекту невдач в різних компонентах і інфраструктурі даної системи.

В роботі розглянуто підходи реагування, що базуються на фіксованих WSN та систем мобільної підтримки. Найбільш перспективним підходом, на думку авторів, є саме система мобільної підтримки, оскільки дозволяє автономно діяти кожному потерпілому. В подальшій роботі планується розробка макету для навігації із застосування БСМ на основі програмованої плати Arduino і радіомодулів XBee.

Література

1. Terrestrial ecology observing systems, center for embedded networked sensing. [Електронний ресурс] – Режим доступу до ресурсу: http://research.cens.ucla.edu/.
2. Providing group tour guide by rfids and wireless sensor networks, IEEE Transactions on Wireless Communications. // 8. – 2009. – №2. – С. 3059–3067.
3 Congestion-aware, loss-resilient bio-monitoring sensor networking for mobile health applications, IEEE Journal on Selected Areas in Communications. // 27. – 2009. – №4. – С. 460–465.
4. Maximal lifetime scheduling for sensor surveillance systems with k sensors to one target, IEEE Transactions on Parallel and Distributed Systems. // 17. – 2006. – №12. – С. 1526–1536.
5. Wireless sensor networks in intelligent transportation systems, Wireless Communications and Mobile Computing. // 9. – 2009. – №3. – С. 287–302.
6. Computers and Mathematics with Applications. // 64. – 2012. – С. 3869–3880.
7. Intelligent Systems and Networks Group, Department of Electrical & Electronic Engineering.

УДК 621.382

ТРИРІВНЕВА АРХІТЕКТУРА ВЗАЄМОДІЇ IOT ПРИСТРОЇВ

Шоферівський А. С., Курдеча В. В.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: goremchik@gmail.com

Three-tier architecture interaction for IoT devices

The three-tier architecture of communicating with many IoT devices is presented. The main idea of this work is that additional routers are implemented: smart sensors transmit collected information to the router, then this router transmits data to the gateway, and then it sends data to the Internet.

Через навантаження на транспортну мережу, що спричиняється великою кількістю IoT пристроїв, за останні кілька років було створено новий підхід до реалізації архітектури таких мереж. Даний підхід передбачає використання дворівневої архітектури мережі IoT пристроїв. В типовій мережі такої архітектури всі розумні датчики підключаються до попередньо налаштованого gateway (шлюза), який забезпечує передачу даних від пристроїв до транспортної мережі (Інтернет).

Згадана реалізація даної архітектури оптимальна при невеликій кількості датчиків. Якщо розглядати випадок, коли кількість IoT пристроїв значно перевищує максимально допустиму, яку може обробити gateway, потрібно або збільшувати кількість gateway, що значно підвищує вартість реалізації такої архітектури, або ж використовувати інший підхід.

У даній роботі пропонується реалізація такого підходу, який би дозволив використовувати архітектуру з багатьма датчиками, при можливості використання лише одного gateway (див. Рис. 1). Це досягається тим, що замість багатьох gateway можна побудувати дану архітектуру використавши додаткові проміжні пристрої – «маршрутизатори». Завдання останніх – прийняти дані від розумних датчиків та перенаправити їх на gateway. Оскільки gateway виконує значно більше функцій, наприклад: підтримка постійного зв’язку із сервером, організація безпечної передачі даних (шифрування інформації) чи локальне збереження даних у випадку відсутності зв’язку із сервером, його вартість значно вище, ніж вартість маршрутизатора, який лише попередньо обробляє дані та передає їх до gateway. Тому оптимальним рішенням буде використання саме

маршрутизаторів, які б об’єднували дані від групи IoT пристроїв та надсилали їх на gateway.

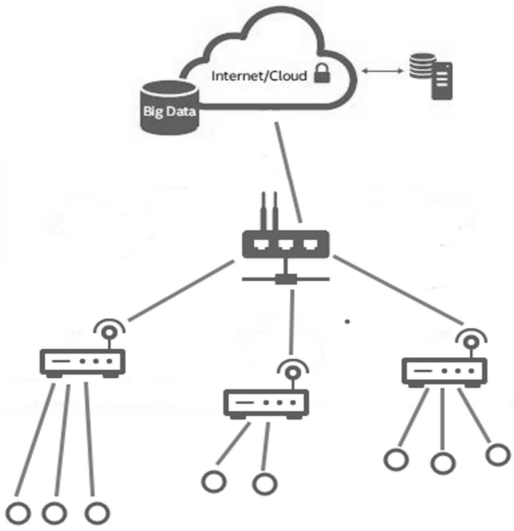


Рис. 1. Трирівнева архітектура взаємодії IoT пристроїв.

Для реалізації прототипу цієї концепції, у якості маршрутизатора можна використовувати мікроконтролер з великою обчислювальною здатністю, наприклад: Arduino Due, Arduino 101, Netduino, але для побудови більш надійного повноцінного пристрою, варто використовувати потужніші мікроконтролери на базі STM-32. Передбачається, що такий мікроконтролер матиме два інтерфейси зв’язку: один для з’єднання із gateway, який має бути налаштований на всіх маршрутизаторах даної мережі однаково, а також інший, який би забезпечував з’єднання із групою IoT пристроїв. Останній інтерфейс підтримує використання різних протоколів і технологій обміну та передачі даних. До таких технологій можна віднести: BLE (Bluetooth Low Energy), Wi-Fi, Zigbee, і навіть дротове підключення пристроїв. Інтерфейс, що забезпечує з’єднання із gateway, зазвичай, реалізовується за допомогою радіоканалу, який обирається таким чином, щоб не інтерферувати з іншими мережами.

У якості кінцевого пристрою не обов’язково використовувати мікроконтролер з великою обчислювальною здатністю. До таких пристроїв можна віднести: Arduino Uno, Arduino Mega, STM-8, а також безліч інших мікроконтролерів, що пропонуються на сучасному ринку. Ці мікроконтролери збирають данні з датчиків, реалізовують їх обробку, автоматизацію деяких процесів та передачу даних чи, навпаки, отримання команд від маршрутизатора (що є транзитним пунктом між кінцевим пристроєм, gateway та користувачем).

Для реалізації gateway, зазвичай, використовуються міні комп’ютери чи потужні мікроконтролери, на які можна поставити операційну систему

(наприклад, Linux-подібну чи Windows 10 IoT). Gateway має 2 інтерфейси зв’язку, один з яких має однакові налаштування з відповідним інтерфейсом маршрутизатора, а інший - кілька варіацій реалізації: Ethernet, GSM, 3G чи Wi-Fi. До функцій gateway відносять:

- Отримання даних від маршрутизаторів;
- Локальне збереження прийнятих даних;
- Шифрування даних;
- Відправка інформації на сервер;
- Прийняття команд з серверу.

Використання такого підходу дає ряд переваг:

- Оскільки на кінцеві пристрої (сенсори) покладається мінімум задач: збір інформації та її передача на маршрутизатор, це зменшує навантаження на сам пристрій, тому його реалізація спрощується, а вартість зменшуються;

- Зменшується навантаження на gateway, тому збільшується стабільність його роботи;

- Використання такого підходу передбачає можливість підключення великої кількості IoT пристроїв на невеликій площі, які виконують абсолютно різні функції і працюють в зовсім різних сферах життя;

- Вирішується важлива проблема захисту інформації, тому що всі сенсори передають інформацію захищеним шляхом, через опцію шифрування на gateway;

- Зменшується можливість втрати даних завдяки опції локального зберігання, що передбачена gateway.

Література

1. Ovidiu Vermesan, Peter Friess (2013). *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*. Aalborg: River Publishers. p7-16.
2. Hao Chen. *A brief introduction to IoT geteway* [Електронний ресурс] / Hao Chen, Xuegin Jia, Heng Li // Proceedings of ICCTA2011. – 2011. – Режим доступу до ресурсу: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6192937.
3. IoT Gateway: *Brifging Wireless Sensor Networks into Internet of Things* [Електронний ресурс] // 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing. – 2010. – Режим доступу до ресурсу: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5703542.
4. Chang-le Zhong. *Study on the IoT Architecture and Gateway Technology* [Електронний ресурс] / Chang-le Zhong, Zhen Zhu, Ren-gen Huang // 2015 14th International Symposium on Distributed Computing and Application for Business Engineering and Science. – 2015. – Режим доступу до ресурсу: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7429590.
5. Курдеча В. В. Метод обновления программного обеспечения в мобильных SDR системах / Л. С. Глоба, В. В. Курдеча. // Научно-технический журнал: "Электроника и связь". – 2008. – №4.

УДК 621.396.946

ПОБУДОВА НАЙКОРОТШОГО РОЗКЛАДУ ЗБОРУ ДАНИХ У БЕЗПРОВОДОВІЙ СЕНСОРНІЙ МЕРЕЖІ З ОБМЕЖЕНИМ КРИТИЧНИМ ЕНЕРГОСПОЖИВАННЯМ

Шпанчук О.О.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: oshpantshuk@gmail.com

Designing Brief Schedule of Data Collectionin Wireless Sensor Network with Limited Energy Consumption

It is presented the algorithm of optimization of data collection in wireless sensor networks with limited critical power, where it is the ability of the direct data transfer between any two nodes. This algorithm is optimal for minimization of time, trees and schedule data collection for WSN.

Основною проблемою використання БСМ є проблема оптимального ЗД. Тому безліч досліджень БСМ спрямовані на створення алгоритмів, що забезпечують збір даних (ЗД) з сенсорних вузлів (СВ)за мінімальний час при мінімальному споживанні енергії (СЕ). Наприклад, в [1] пропонується варіант адаптивного розкладу передач даних (кожен вузол сам складає свій розклад виходячи з спостережуваного поведінки сусідніх вузлів). Однак, в більшості випадків [2], завдання зводиться до складання постійного розкладу СД. Різні дослідники формулюють завдання складання розкладу по-різному, включаючи або не включаючи до неї різні чинники, беруть за основу різні варіації БСС. Наприклад, в [4] вважається, що відомі географічні координати вузлів. В [3] розглядаються мобільні БСС, в яких вузли можуть переміщатися в просторі. У даній статті пропонується своєрідний підхід, заснований на побудові дерев ЗД за образом і подобою ідеальних дерев ЗД для ідеальних БСМ (в яких можлива пряма передача даних між будь-якими двома вузлами).

ЗД в БСМ здійснюється циклами, тривалість яких рівна між собою. Цикл складається з часових інтервалів (ЧІ), протягом яких вузли передають один одному дані. Щоб уникнути колізій, кожен вузол протягом одного ЧІ обмінюється даними не більше ніж з 1 вузлом. Очевидно, що протягом одного циклу не має сенсу передавати дані більш ніж один раз.

Мінімізуючи СЕ мережі, можна говорити про мінімізацію максимального (критичного) СЕ серед всіх СВ мережі. Так як ємність автономних ДЖє однаковою у всіх СВ, то критичним фактором є мінімізація максимального числа передач серед усіх СВ мережі протягом одного циклу.

Так як СЕ кожного вузла однозначно визначається деревом, то при складанні розкладу передач даних по наявному дереву, оптимізація здійснюється лише за одним критерієм - за часом ЗД. Мінімізація часу досягається за допомогою скупого алгоритму, суть якого полягає в ЗД на кожному кроці (ЧІ) з максимально можливого числа вузлів. Такий алгоритм дій оптимальний, так як кожен вузол, перш ніж передати дані, повинен здійснити

прийом даних від усіх своїх синів по дереву збору, а, отже, черговість, в якій відбувається прийом даних від синів, не має значення.

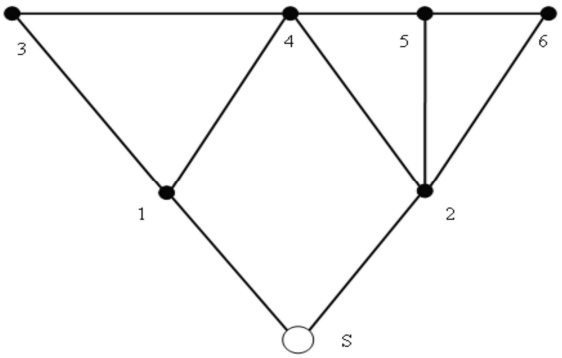


Рис. 1. Граф БСМ

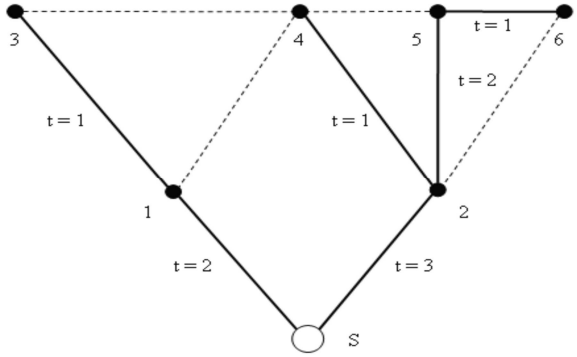


Рис. 2 Оптимальне дерево ЗД для БСМ із рис. 1

Розглянемо БСМ, показану на рис. 1, і відповідне їй дерево ЗД (рис. 2), де пунктирними лініями позначені ребра графа БСМ, які не ввійшли в дерево ЗД. На обох рисунках позначення «S» відповідає вузлу. Отже, на першому кроці вузли 3, 4 і 6 передають дані до вузлів 1, 2 і 5, відповідно. На другому кроці вузли 1 і 5 здійснюють передачу вузлів S (центральний вузол) і 2, відповідно. На останньому - третьому кроці, вузол 2 передає дані в центральний вузол, на цьому цикл ЗД завершується. Таким чином, час ЗД в даному прикладі становить 3 ЧІ, в той час як критичне енергоспоживання дорівнює 2 (вузол 2 має 2 синів - вузли 4 і 5).

Щоб по заданому зв'язаному графу БСМ, побудувати дерево ЗД з критичним СЕ, що не перевищує заданого та забезпечує мінімальну довжину циклу ЗД, розглянемо випадок, коли БСМ задана повним графом, тобто $\forall u, v \; \exists (u,v) \in E$, де $u, v \in V$. Тому між будь-якими двома вершинами графа $G = (V, E)$ існує ребро. Отже, про БСМ досить знати лише число вузлів n.

Нехай $f_s(t, e)$ - максимальне число вузлів ідеальної БСМ з часом ЗД t із критичним СЕ меншим або рівним e, тоді для вирішення нашої задачі досить знайти такий мінімальний час t, при якому функція $fs(t, e) \geq n$, і$fs(t, e)$зростаюча по t при фіксованому e, тому шукане значення t можна визначити будь-яким відомим алгоритмом пошуку для монотонних функцій, наприклад, двійковим пошуком;$fs(t, e)$ знаходимо за формулою:

$$fs(t, e)=\sum_{i=1}^{t} fp(t-i, e),$$

де$fp(t, e) = \sum_{i=1}^{\min(t,e)} fp(t-i, e)$

Функція fs застосовується для центрального вузла, а fp– для сенсорного. Таким чином, враховується той факт, що СЕ центрального вузла не впливає на критичне СЕ мережі. Функції fs і fp коректні, так як, якщо з усіх вузлів деякого піддерева дерева ЗД потрібно зібрати дані за час t, то максимальний припустимий час ЗД для безпосередньо дочірнього вузла кореня піддерева рівний t-1, коли t-1 «віддано» одному з таких вузлів, максимально допустимий час що залишилися стає рівним t-2 і т.д.

На рис. 3 представлено ідеальне дерево ЗД, побудоване згідно функції *fs*(5, 2), тобто дерево з критичним СЕ *e* = 2 і максимальним числом вершин, за яким можливо здійснити ЗД за час t = 5. Дерево містить 27 вершин. На першому кроці (ЧІ) дані передають вузли 1-12, на другому - вузли 13-19, на 3-му - 20-23, на 4-му - 24-25, на 5-му - 26.

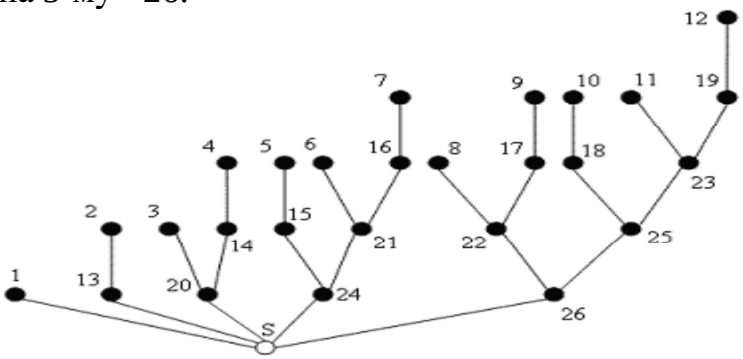


Рис. 3. Ідеальне дерево збору даних для *t* = 5, *e* = 2

Дерево ЗД найбільш близьке по топології ідеального дерева будується ітеративно від кореня (центрального вузла БСМ) до листів в 2 кроки, при чому, другий крок виконується після першого.

На першому кроці спочатку випадковим чином вибирається вершина u, вже включена в дерево (спочатку в дерево включена тільки 1 вершина - центральний вузол), потім, також випадковим чином, вибирається вершина v, яка невключена в дерево. Вибір здійснюється так, щоб виконувалися 2 умови:1) між u і v існує ребро в графі БСС; 2) включення v в множину синів u не порушить структури ідеального дерева СД. Етап завершується як тільки або всі вершини потраплять в дерево або не знайдеться таких u і v, для яких виконуються зазначені вище умови.

Крок 2 аналогічний кроку 1, з тією лише відмінністю, що вузли u і v повинні відповідати лише умові 1. Етап завершується як тільки всі вершини будуть включені в дерево.

Таким чином, всі вершини графа БСМ будуть включені в дерево ЗД. Описаний алгоритм виконується k раз, серед знайдених рішень вибирається краще.

Створення алгоритмів, заснованих на запропонованому підході, оптимізованих для графів із специфічною топологією дозволить досягати високих результатів, максимально близьких до глобального оптимуму, особливо на насичених графах.

Література

1. Sharat C. Visweswara, Rudra Dutta, Mihail L. Sichitiu, Adaptive ad-hoc self – organizing scheduling for quasi-periodic sensor network life time, Computer Communications 29 (2006), 3366–3384.
2. Shen, Y. -J., &Wang, M.-S., Broadcast scheduling in wireless sensor networks using fuzzy Hopfield neural network, Expert Systems with Applications 2 (2007), 900–907.
3. Yaoyao Gu, Doruk Bozdag, Robert W. Brewer, Eylem Ekici, Data harvesting with mobile elements in wireless sensor networks, Computer Networks 50 (2006), 3449–3465.
4. Shibo Wu, K. Selcuk Candan, Power-aware single- and multipath geographic routing in sensor networks, AdHoc Networks 7 (2007), 974-997.

УДК 621.396.946

МЕТОДИ ЗАБЕЗПЕЧЕННЯ СТІЙКОЇ РОБОТИ СЕНСОРНИХ МЕРЕЖ НА БАЗІ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Явіся В.С.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: yavisya@bigmir.net

Methods to ensure sustainable operation of sensor networks based on unmanned aerial vehicles

Quality work sensor networks when using unmanned aerial vehicles (UAV) is possible only when the exact positioning of the UAV in space. Discusses the problematic aspects and possible methods to solve this problem, including when deploying their own navigation system based on grouping of nanosatellites.

Якісна робота сенсорних мереж залежить від варіанта реалізації телекомунікаційної складової, що у більшості застосувань таких мереж повинна забезпечити підтримку мобільності сенсорів, а також своєчасну доставку інформації від них. Виконання таких вимог можливо при використанні безпілотних літальних апаратів (БПЛА). У цьому випадку необхідно вирішувати завдання, пов'язані із забезпеченням руху БПЛА по обумовленій поточними умовами траєкторії. Успішне рішення такого завдання фактично гарантує виконання сенсорною мережею покладених на неї функцій у повному обсязі. Однак, на жаль, саме тут можуть виникнути труднощі, зв'язані зі стабільністю каналу керування БПЛА. У найгіршому випадку, тобто при відсутності керування, здійснюється перехід на автономний режим польоту, організований відповідно до закладеного алгоритму по заданій заздалегідь траєкторії. У свою чергу його ефективна реалізація можлива, як правило, тільки за умови точного позиціювання БПЛА в просторі.

В загалі, остання умова буде виконаною при реалізації одного з аспектів процесів глобалізації світової економіки, що складається в поетапному створенні до 2025 року світової аеронавігаційної системи відповідно до Глобальної експлуатаційної концепції Міжнародної організації цивільної авіації ICAO (від англ. ICAO – International Civil Aviation Organization). Передбачається, що Росія й США, будучи глобальними гравцями, здійснять інтеграцію своїх аеронавігаційні системи у світову, що припускає перехід до перспективної техніки й технологій концепції CNS/ATM (від англ. Communication, Navigation and Surveillance/Air Traffic Management – зв'язок, навігація, спостереження/організація повітряного руху) [1].

В теперішній час вимоги CNS/ATM орієнтовані на використання на всіх етапах польоту повітряних судів (ПС) Глобальних навігаційних супутникових систем GNSS (від англ. GNSS – Global Navigation Satellites System) с поступовим усуненням потреби в наземних засобах [2].

Системи аеронавігації GNSS (GPS, ГЛОНАСС й ін.) дозволяють визначати координати об'єктів на великих територіях з високою точністю. Їх можливості значно ширше, ніж у систем на базі наземних засобів. Однак застосування супутникової навігації GNSS як єдиного засобу одержання аеронавігаційної інформації несе в собі значні ризики, що може відбитися на безпеці польотів, стабільності перевезень, а також роботі сенсорних мереж, що базуються на БПЛА. До основного із цих ризиків можна віднести наступні [3]:

• у силу енергетичної слабості прийнятих навігаційних сигналів абонентські термінали GNSS уразливі для постановників активних радіоперешкод, як навмисних, так і ненавмисних;

• монополізація володінням GNSS (GPS, ГЛОНАСС – військові відомства) не виключає того, що доступна точність навігаційних показників може бути навмисно погіршена, навігаційні сигнали можуть бути закодовані або навіть відключені при зміні міжнародної обстановки;

• внаслідок глобального характеру GNSS локальний вплив на окремі елементи систем (космічні апарати, наземні пункти керування й ін.) здатний унеможливити використання авіації й систем керування повітряним рухом у значній частині земної кулі.

Для нейтралізації можливих негативних наслідків необхідна наявність альтернативних GNSS засобів, використовуваних у якості основних, додаткових або резервних.

При цьому, з урахуванням положень CNS/ATM, вони повинні відповідати наступним основним вимогам [2]:

• мати аналогічними з GNSS функціональними можливостями по забезпеченню навігації;

• точність визначення місця розташування повинна бути не гірше, ніж у систем, побудованих на базі GNSS;

• бути повністю незалежними від даних GNSS;

• забезпечувати можливість інтеграції з перспективними системами на базі GNSS для поліпшення показників точності, цілісності, безперервності й експлуатаційній готовності в різних територіальних районах.

На 12-й Аеронавігаційній конференції ICAO (Монреаль, Канада, 19-30 листопада 2012 р.) було заявлено про необхідність створення альтернативних стосовно GNSS наземних засобів аеронавігації. Однак у цей час, на ринку системи такого класу поки не представлені.

Значне зниження впливу зазначених негативних факторів досягається шляхом реалізації ряду дій, що включають застосування [3]:

- комплексу спеціально розроблених алгоритмів, що базуються на нових комбінованих способах визначення просторових координат у багатопозиційних системах;

- спеціальних методів синхронізації системи без використання модулів атомного еталона часу й координат часу GNSS;

- оптимального просторового конфігурування радіомаяків;

- складних сигналів із заданими індивідуальними ознаками;

- сучасної електронної компонентної бази, що забезпечує мінімізацію вагогабаритних характеристик устаткування й високу обчислювальну потужність вирішальних пристроїв;

- технології створення бортових багатофункціональних приймачів, сполучених з обладнанням GNSS, що дозволяє звести до мінімуму обсяг необхідних конструктивних доробок на борту ПС, а в деяких випадках забезпечити їх повну відсутність.

Наземні засоби аеронавігації, будучи альтернативою системам GNSS, все ж таки не зможуть виконувати свої функції в умовах потужних радіоперешкод. Крім того їх ефективне застосування є обмеженим деякою просторовою областю.

Для переважної більшості країн світу реальною загрозою залишається варіант втрати навігаційних сигналів у випадку їхнього відключення або кодування відповідними монополістами GNSS (наприклад GPS, ГЛОНАСС).

Очевидно, що в даній ситуації залишитися незалежним від GNSS можна при розгортанні власної навігаційної системи. Така можливість з'являється, коли мова йде про використання угруповання наносупутників (НС). Завдяки їх відносно невисокої вартості створення й виводу на орбіту, кількість елементів такої системи може бути досить великою, що за умови забезпечення синхронізації випромінюваних сигналів дозволить створити їх достатній енергетичний рівень на вході приймача, навіть в умовах застосування активних навмисних радіоперешкод.

У складної, стосовно наявності перешкод, обстановці, за умови використання спрямованих антен на борту НС, значно збільшити енергетику навігаційних сигналів у заданій області також можливо шляхом рішення завдання забезпечення необхідного керованого просторового положення НС. Існуючі методи й способи орієнтації й стабілізації, які можна застосувати до НС, найчастіше не дозволяють досягти необхідної точності просторового положення. Однак, можливим рішенням у даній ситуації є застосування методів теорії оптимального керування.

Таким чином, для забезпечення стійкої роботи сенсорних мереж на базі БПЛА, а також незалежності України в сфері аеронавігації, досить перспективним напрямком є розгортання власної навігаційної системи, що базується на угрупованні НС, за умови рішення завдань синхронізації випромінюваних сигналів, орієнтації й стабілізації просторового положення НС із необхідною точністю.

Література

1. Doc. 9750-AN/963. Глобальный аэронавигационный план применительно к системам CNS/ATM. – Изд. 2-е. – Монреаль: ICAO, 2002.
2. Системы CNS/ATM: учеб. пособие / Сост. В.А. Казаков. – 2-е изд., перераб. и доп. – Ульяновск: УВАУ ГА, 2008. – 103 с.
3. Кузьминский А.В. Вопросы создания новых систем аэронавигации // Мобильные телекоммуникации – № 2 – М.: «Профи-Пресс», 2014. – С. 10-11.

УДК 621.395

МЕТОДИКА ВИБОРУ МОВНИХ КОДЕКІВ

Явіся В.С.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: yavisya@bigmir.net

The method of selecting language codecs

Quality of language significantly depends on the type and the method of constructing network and algorithm of encoding of verbal information-codec. Each codec is described by a set of quality indicators, which are interdependent and contradictory and have quite different units of measurement. The proposed simplified algorithm comparison and choice of language for the codec on the aggregate indicators.

Якість передачі мови істотно залежить як від типу та способу побудови мережі, так і від алгоритму кодування мовної інформації – кодека. Тому, ще на етапі проектування мережі необхідно визначитись – який мовний кодек буде застосований.

Всі існуючі типи мовних кодеків за принципом дії можна розділити на три групи [1]:

- Кодеки з імпульсно-кодовою модуляцією (ІКМ, Pulse Code Modulation – PCM) і адаптивною диференціальною імпульсно-кодовою модуляцією (АДІКМ, Adaptive differential pulse-code modulation – ADPCM).
- Кодеки з вокодерним перетворенням мовного сигналу.
- Комбіновані (гібридні) кодеки.

Показники якості мовних кодеків взаємозалежні й суперечливі. Часто кодеки описують п'ятьма показниками якості: k_1 – швидкість кодування, k_2 – оцінка якості кодування мови, k_3 – складність реалізації, k_4 – сумарна затримка, k_5 – розмір кадру [2].

Швидкість кодування визначає вимоги до пропускної здатності каналу.

Оцінка якості кодування мови з використанням різних кодеків здійснюється за допомогою характеристики MOS (Mean Opinion Score), це усереднена сукупна думка по 5-бальній шкалі.

Складність алгоритму кодування пов'язана з необхідними обчисленнями в реальному часі. Складність алгоритму визначає швидкість обробки, вимірювану в мільйонах операцій у секунду (Million Instructions Per Second, MIPS). Складність обробки впливає на фізичні розміри кодуючого, декодуючого або комбінованого пристрою, а також на його вартість і споживану потужність.

Часова затримка збільшується зі збільшенням розміру кадру, а також зі збільшенням складності алгоритму кодування. При передачі мови припустима затримка в одному напрямку не може бути більше 250 мс.

Оскільки розмір кадру з однієї сторони впливає на якість відтвореної мови, а з іншого боку – на затримку переданої інформації, пов'язану з обробкою, то такий показник можна виключити, врахувавши його значення шляхом корегування k_2, k_4.

Більшість кодеків описані рекомендаціями сімейства «G» стандарту H.323 [3]. Їх основні характеристики наведені в таблиці 1. Вибір алгоритму кодування мови залежить від вимог до якості, характеристик каналу, що є у розпорядженні, можливостей реалізації певного алгоритму з погляду на складність обчислень.

Запропонований в [4, 5] спосіб вибору варіанта мовного кодека методом аналізу ієрархій складається в декомпозиції проблеми вибору єдиного варіанта системи на прості складові частини й одержанні чисельних даних суджень експертів по парних порівняннях різних елементів проблеми вибору. У результаті обробки отриманих даних виходять оцінки компонентів вектора глобальних пріоритетів, що характеризує пріоритетність порівнюваних варіантів системи.

Таблиця 1. Основні характеристики кодеків.

Кодек	**Метод компресії**	**Швидкість кодування (k_1)**	**Якість, MOS (k_2)**	**Складність реалізації (k_3)**	**Затримка (k_4)**
G.711	PCM	64 Кбіт/с	Висока 4,1	Низька (8 MIPS)	Дуже низька (0,75 мс)
G.726	ADPCM	32/24/16 Кбіт/с	Середня 3,96 (32 Кбіт/с), Погана 3,12 (16 Кбіт/с)	Низька (8 MIPS)	Дуже низька (1 мс)
G.729	CS-ACELP	8 Кбіт/с	Середня 3,92	Висока (30 MIPS)	Низька (10 мс)
G.729A	CA-ACELP	8 Кбіт/с	Середня 3,7	Помірна (20 MIPS)	Низька (10 мс)
G.723.1	MP-MLQ ACELP	6,4/5,3 Кбіт/с	Середня 3,87 (6,4 Кбіт/с), Середня 3,69 (5,3 Кбіт/с)	Помірна (16 MIPS)	Висока (37 мс)
G.728	LD-CELP	16 Кбіт/с	Середня 3,61	Дуже висока (40 MIPS)	Дуже низька (3-5 мс)

Для одержання вектора глобальних пріоритетів порівнюваних варіантів мовних кодеків із залученням суджень досвідчених експертів на кожному рівні ієрархії формується й виконується обробка матриць парних порівнянь альтернатив.

Компоненти головного власного вектора матриці парних порівнянь обчислюються як середнє геометричне значення в рядку матриці парних порівнянь, а компоненти вектора пріоритетів обчислюються як нормовані значення компонентів головного власного вектора.

Пропонується деяке спрощення процедури вибору єдиного варіанта кодека в порівнянні з викладеним в [4, 5] методом. Сам процес вибору буде складатися із двох етапів. На першому виконується приведення показників до однотипного характеру і їх нормування, на другому – безпосередньо обчислення абсолютних значень оцінок кожного кодека. Результати

заносяться в таблицю 2.

У нижньому рядку зазначені вагові коефіцієнти (значимість) p_i відповідного показника, які визначаються досвідченими експертами на основі даних про проектовану мережу.

Абсолютна оцінка S для кожного кодека обчислюється відповідно до виразу:

$$S = \sum_{i=1}^{4} k_{i\text{н}} \times p_i,$$

де $k_{i\text{н}}$ – перетворені нормовані показники якості кодека;

p_i – вагові коефіцієнти відповідних показників якості кодека.

Пріоритет віддається кодеку, що має найбільше значення абсолютної оцінки.

Таблиця 2. Результати обчислень абсолютних оцінок кодеків.

Кодек	**Показники якості**				**Абсолютна оцінка кодека**
	Швидкість кодування ($k_{1\text{н}}$)	**Якість, MOS ($k_{2\text{н}}$)**	**Складність реалізації ($k_{3\text{н}}$)**	**Затримка ($k_{4\text{н}}$)**	
G.711	0,10	1,00	1,00	1,00	0,58
G.726	0,20	0,97	1,00	0,75	0,59
G.729	0,80	0,96	0,27	0,08	0,71
G.729A	0,80	0,90	0,40	0,08	0,71
G.723.1	1,00	0,94	0,50	0,02	0,83
G.728	0,40	0,88	0,20	0,19	0,50
Вагові коефіцієнти	0,47	0,30	0,15	0,08	

Запропонований алгоритм вибору мовного кодека дає результати, аналогічні описаному в [5], але потребує меншої кількості обчислювальних процедур.

Література

1. Росляков А.В., Самсонов М.Ю., Шибаева И.В. IP-телефония. – М.: Эко-Трендз, 2003. – 251с.
2. Семенов Ю.В. Проектирование сетей связи следующего поколения. – СПб.: БХВ-Петербург, 2005. – 236 с.
3. Рекомендації ITU-T H.323.
4. Саати Т., Кернс К. Аналитическое планирование. Организация систем. – М.: Радио и связь, 1991. – 224 с.
5. Безрук В.М. Методы многокритериальной оптимизации при выборе речевых кодеков с учетом совокупности показателей качества [Электронный ресурс] / В.М. Безрук, Ю.В. Скорик, Д.В. Чеботарёва // Проблеми телекомунікацій. – 2013. – № 3 (12). – С. 27-35. – Режим доступа к журн.: http://pt.journal.kh.ua/2013/3/1/133_bezruk_optimization.pdf .

УДК 621.391

МЕТОД ПІДВИЩЕННЯ АБОНЕНТСЬКОЇ ЄМНОСТІ СИСТЕМ МОБІЛЬНОГО ЗВ'ЯЗКУ

Явіся В.С.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: yavisya@bigmir.net

Methods to increase subscriber capacity of base stations of mobile communication

Reasonable possibility of increasing the subscriber capacity of base stations of mobile communication systems, as well as solving the overload problem, the base stations with large number of subscribers in a limited area of convergence through UMA technology with simultaneous introduction of modernized subscriber terminals.

Останнім часом продовжується процес стрімкого зростання потреб користувачів у наданні інфокомунікаційних послуг, причому незалежно від способів абонентського доступу. За останні роки це викликало процес конвергенції телекомунікаційних та інформаційних мереж, побудованих за різними принципами. Однак, як завжди, Оператори повинні пам’ятати про необхідність забезпечення заданих показників якості обслуговування. Існуючи традиційні методи доступу рухомих абонентів до мережних ресурсів дозволяють успішно вирішувати цю задачу лише за умови перебування в зоні обслуговування (ЗО) базової станції (БС) певного числа абонентів, що вимагають обслуговування. При перевищенні цього нормативного значення відбувається значне погіршення показників якості обслуговування. В зв’язку із постійним зростанням кількості мобільних користувачів Оператори повинні постійно займатися модернізацією мережі. Основними напрямками такої діяльності є встановлення додаткових БС із меншим радіусом ЗО, збільшення кількості секторів БС, застосування технології MIMO у сполученні із адаптивними антенами. Звичайно ж що це потребує від Оператора значних капіталовкладень. Крім того, технологічно обмежені можливості мереж доступу GSM, WCDMA, та навіть WiMax і LTE стають стримуючим чинником на шляху впровадження нових сервісів.

Зазначені чинники обумовлюють необхідність пошуку додаткових шляхів забезпечення зростаючої кількості користувачів інфокомунікаційними послугами із заданими показниками якості обслуговування.

В цьому сенсі варто згадати можливість оптимізації мережної інфраструктури мобільного Оператора шляхом перерозподілу мережних ресурсів, наприклад із застосуванням Wi-Fi доступу, який вже мається в межах ЗО БС, або додатково встановлюється Оператором безпосередньо в місці розташування БС, або там, де прогнозується скупчення великої кількості абонентів.

Конвергенція сучасних технологій надає можливість ефективного використання існуючих канальних ресурсів. Вартість частотного каналу Wi-Fi нижча, ніж ресурсів мереж GSM/WCDMA/WiMax/LTE. Отже використання цієї

технології у поєднанні з комірковими мережами дає змогу знизити собівартість послуг зв'язку, які надаються клієнтові Оператора зв’язку.

Інтерес Операторів мобільного зв'язку до сегмента безпроводового широкосмугового доступу проявився доволі давно й спочатку був пов'язаний скоріше з наданням послуг доступу в Інтернет за технологією Wi-Fi, ніж із здатністю забезпечити абонентів унікальним набором можливостей і послуг. У випадку надання конвергентних послуг Оператором мобільного зв'язку "з одних рук" – різко підвищується привабливість такої мережі для клієнтів, крім того рішення виявляється безумовно ефективним і з економічної точки зору [1].

Концепція побудови конвергентної телекомунікаційної мережі викликала прийняття союзом 3GPP у квітні 2005 року специфікації технології Unlicensed Mobile Access (UMA — не ліцензований мобільний доступ). UMA – це розроблений низкою провідних компаній-виробників та Операторів стандарт абонентського доступу до сервісів мереж мобільного зв'язку за допомогою IP-мереж. Спочатку стандарт створювався для підключення до коміркових мереж за допомогою технології Wi-Fi. По мірі розвитку UMA стає вдосконаленим універсальним мобільним доступом за рахунок використання контролера, який здійснюватиме інтеграцію мереж Wi-Fi з різними поколіннями мереж мобільного зв’язку. Технологія UMA дає можливість використання широкосмугового безпроводового Інтернет-з’єднання (Wi-Fi) для забезпечення доступу до систем мобільного зв’язку. Це стосується голосових викликів, мобільного Інтернету, електронної пошти та будь-яких інших мобільних послуг, для яких необхідне підключення до існуючих мобільних мереж [2].

Передбачається, що модернізований абонентський термінал самостійно визначає можливість отримання послуг через одну з мереж (GSM/WCDMA/ WiMax/LTE/Wi-Fi), при цьому пріоритет надається мережі, яка забезпечує вищий рівень якості надання послуг, а її вибір здійснюють контролер у Wi-Fi мережі і контролер базових станцій Оператора мобільного зв’язку. Модернізація терміналу можлива програмним шляхом без зміни його апаратної частини. Wi-Fi точки доступу підключені до існуючої транспортної IP-мережі, яка у свою чергу під'єднується до контролера UMA Network Controller (UNC), що ввімкнений у Mobile Switching Centre (MSC – центр мобільної комутації). Шлюзування між MSC та UNC відбувається через шлюзи Wireless Media Gateway (WMG) – для підтримки голосової несучої UMA, та Security Gateway (SeGW) – шлюз безпеки для захисту UMA. На UNC відбувається пакетування та кодування голосу при роумінгу, наприклад Wi-Fi/GSM, та розпакування і декодування при зворотній передачі.

Функції UNC еквівалентні функціям, що виконуються контролером базових станцій мережі стільникового зв'язку. Контролер підключається до точки доступу WLAN через транспортне сполучення IP. З мобільною станцією контролер UNC взаємодіє через інтерфейс, який в свою чергу функціонує через транспортну мережу IP і здійснює перенесення сигналізації GSM/WCDMA/ WiMax/LTE між опорною мережею і мобільною станцією. Протокольні дані мобільних мереж переносяться прозоро між мобільною станцією і MSC. Це забезпечує мобільній станції в мережі WLAN доступ до всіх послуг мережі GSM, які їй можуть бути доступні у підсистемі базових станцій мережі GSM.

Під час дзвінків всередині Wi-Fi пакети не залишають IP-мережі, а під час викликів у межах GSM/WCDMA/WiMax/LTE в якості транспорту використовується існуюча транспортна мережа Оператора [2].

Реалізація хендовера у процесі інтеграції мереж GSM/WCDMA/ WiMax/LTE і безпроводової Wi-Fi мережі здійснюється наступним чином:

• мобільний абонент із терміналом UMA потрапляє в зону дії мережі не ліцензованого безпроводового доступу, з якою цей термінал UMA взаємодіє;

• після підключення терміналу UMA до точки доступу він зв'язується з контролером UNC по транспортній IP-мережі для автентифікації, авторизації і доступу до послуг мобільного зв'язку по безпроводовій мережі не ліцензованого доступу;

• у разі успішної авторизації відбувається оновлення інформації про місцезнаходження абонента, яка зберігається в опорній мережі;

• залежно від конфігурації терміналу UMA мобільний зв'язок встановлюється або з не ліцензованою мобільною мережею доступу UMA або з мережею GSM/WCDMA/WiMax/LTE;

• коли абонент UMA виходить із зони покриття мережі не ліцензованого безпроводового доступу, до якої він підключений, UNC і термінал UMA забезпечують роумінг з ліцензованою мобільною мережею. Цей процес відбувається автоматично і непомітно для користувача;

• якщо абонент встановив активне з'єднання GSM або LTE і, не перериваючи його, увійшов в зону покриття (або вийшов із зони покриття) не ліцензованої безпроводової мережі, поточне з'єднання автоматично перемикається на іншу мережу без переривання послуги. Хендовер також відбувається непомітно для користувача [2].

Таким чином підвищення абонентської ємності систем мобільного зв'язку, а також вирішення проблеми перевантаження БС при скупченні великої кількості абонентів на обмеженій території, можна здійснити шляхом конвергенції UMA технології із одночасним впровадженням модернізованих абонентських терміналів.

Література

1. Климаш М.М., Лаврів О.А., Бугиль Б.А.. Вплив властивостей трафіку на параметри якості обслуговування вузла мультисервісної мережі // 4-й Международный радиоэлектронный форум "Прикладная радиоэлектроника. Состояние и перспективы развития" МРФ-2011. Сборник научных трудов. Том II. Международная конференция "Телекоммуникационные системы и технологии". – Харьков: АНПРЭ, ХНУРЭ, 2011. – С. 315-318.
2. Климаш М.М. Підвищення якості обслуговування в конвергентних мобільних системах на основі платформи UMA-A [Електронний ресурс]/ М.М. Климаш, М.І. Бешлей, Б.М. Стрихалюк, Г.В. Холявка // Проблеми телекомунікацій. – 2014. – № 1 (13). – С. 3 - 19. – Режим доступу до журн.: http://pt.journal.kh.ua/2014/1/1/141_klymash_uma.pdf.

УДК 520.6.05

СПОСОБЫ УПРАВЛЕНИЯ ПРОСТРАНСТВЕННЫМ ПОЛОЖЕНИЕМ НАНОСПУТНИКА

Явися В.С.
Институт телекоммуникационных систем НТУУ «КПИ», Украина
E-mail: yavisya@bigmir.net

A method of controlling the spatial location of nano-satellites

The analysis of methods of orientation and stabilization of the spatial position of the ultra-small spacecraft. Traditional methods of orientation and stabilization are measured in terms of their feasibility, taking into account the restrictions on weight and overall performance, operational constraints associated with the consumption of energy here, as well as the possibility of changing orbit.

Наноспутники (НС) − перспективный вид космической техники. Такие аппараты весят всего несколько килограммов и могут выводиться в космос в качестве попутной нагрузки или сразу пакетами в десятки и даже сотни единиц. Кластеры спутников могут использоваться в качестве ретрансляционной сети, для дистанционного зондирования Земли, научных миссий, экологического мониторинга, прогноза землетрясений, исследования ионосферы, в том числе полетов к другим планетам. Между тем развитие этой перспективной отрасли сильно сдерживается из-за отсутствия дешевой и эффективной двигательной установки, расширяющей функциональность НС и делающей их по-настоящему автономными устройствами.

В большинстве случаев НС не могут менять свое положение в пространстве, не говоря уже о разгоне и маневрировании в глубоком космосе. Это связано с жесткими массо-габаритными ограничениями, которые вынуждают отказаться от оснащения НС системами стабилизации и ориентации. Однако ряд применений НС возможен только в случае решения задачи обеспечения стабильного, изменяемого положения НС в пространстве.

Известно, что при нахождении на орбите спутник подвергается возмущающим моментам, поэтому даже в случае обеспечения правильной ориентации при выводе на орбиту, через некоторое время возникает необходимость управления его положением.

Традиционно для решения задачи ориентации и стабилизации применяются два метода [1]: пассивный и активный.

Пассивный метод не требует затрат энергии, запасаемой на борту спутника. Наиболее распространены следующие пассивные методы стабилизации: гравитационный, аэродинамический, давлением солнечных лучей, вращением.

Активные методы стабилизации бывают трёх типов:

– стабилизация с помощью двигателей-маховиков;

– стабилизация с помощью моментного магнитопривода;

– система стабилизации с реактивными двигателями.

Возможность применения одной из перечисленных систем стабилизации зависит от совокупности требований, предъявляемых к НС.

В том случае, когда НС решает задачи, не связанные с необходимостью изменять его пространственное расположение на протяжении всего срока эксплуатации, целесообразно использовать пассивные методы.

В остальных случаях обоснованным будет применение активных методов, поскольку именно они помимо стабилизации способны обеспечить изменение ориентации в течении коротких интервалов времени.

Основным преимуществом систем стабилизации с помощью двигателей-маховиков и моментного магнитопривода является то, что они не требуют наличия на борту запасов топлива.

Базирующиеся только лишь на двигателях-маховиках, либо только на магнитных исполнительных органах системы, в принципе способны выполнить необходимую стабилизацию и ориентацию [2].

При использовании двигателей-маховиков необходимо иметь по одной оси два двигателя-маховика, кинетические моменты которых направляются в противоположные стороны. В совокупности шесть таких элементов (по два на каждой из трех осей), займут внутренний объем таким образом, что расположение других элементов НС станет значительно усложненным.

Если ограничить массу системы стабилизации на уровне 10% от массы всего НС, тогда за одну секунду угол поворота НС составит $\alpha_{нс} = 0{,}57$ рад. В целом такая система при незначительном энергопотреблении для работы электродвигателей (до 1 Вт) показывает достаточно высокую эффективность и быстродействие. Основным недостатком такого решения является то, что после окончания ориентации необходимо поддерживать скорость вращения маховиков на заданном значении. При отсутствии достаточного запаса электроэнергии (при нахождении НС в тени) ресурса аккумуляторов может оказаться недостаточно для обеспечения работы электродвигателей, что в свою очередь вызовет потерю ориентации.

Когда речь идет о реализации системы на магнитных исполнительных органах, также можно достичь соотношения массы магнитных катушек на уровне 10% от полезной нагрузки [2, 3].

При использовании магнитных катушек, взаимодействующих с магнитным полем Земли, за секунду угол поворота НС составит $\alpha_{нс} = 0{,}00048$ рад.

Явным преимуществом такой системы является удобство расположения ее элементов в корпусе НС, а именно – сразу под внешними плоскостями сторон куба. Это не будет создавать никаких неудобств при размещении другого оборудования. Кроме того, по окончанию ориентации и стабилизации, система не требует дополнительных энергозатрат.

Недостатками системы на магнитных исполнительных органах является относительно малая величина управляющих моментов, а также то, что без

привлечения дополнительного управляющего устройства другого вида моментный магнитопровод не в состоянии обеспечить трехосную ориентацию НС в пространстве [4].

Реактивные двигатели создают управляющий момент за счет реакции струй газов, истекающих из сопла, ось которого располагается на некотором удалении относительно центра масс НС. Наиболее эффективным будет их расположение на краю поверхности посередине грани.

Общим недостатком таких систем является ограниченное время функционирования в связи с израсходованием рабочего тела. Сам принцип эжекции массы приводит к необходимости создания ее резерва, что утяжеляет НС при запуске.

В этом случае возможно использование ионных двигателей, основным достоинством которых считается экономичность. Так как ионы имеют скорость на порядок выше скорости истечения газов из ракетного двигателя, то для изменения скорости НС на заданную величину им требуется на порядок меньше топлива.

В тоже время использование ионных двигателей связано со значительным потреблением электрической мощности и вызывает необходимость введения фазы предварительного нагрева, что, как правило, удерживает специалистов от их использования для управления положением.

Кроме того недостатком ионных двигателей является очень маленькая тяга, которая не позволяет использовать их для взлета с Земли, а также при маневрах, требующих быстрого изменения траектории.

Однако нанодвигателестроение не стоит на месте [5]. Как было заявлено в пресс-релизе Массачусетского технологического института, группой американских инженеров были разработаны специальные сверхкомпактные ионные двигатели для коррекции орбиты НС.

Габариты ионного ускорителя составляют 10х10х2 мм.

Запас топлива, или другими словами реактивная масса, будет храниться непосредственно внутри двигателя в жидком виде и поступит наружу через микроскопическое отверстие, где ее частицы ионизируются и ускоряются электрическим полем.

Группа разработчиков, возглавляемая Государственной политехнической школой в Лозанне и входящая в европейский консорциум по созданию электрических ракетных микродвигателей MicroThrust, заявила о создании первого рабочего прототипа ультракомпактного космического двигателя нового поколения, использующего технологию матричных микросопел [6].

Созданный европейцами рабочий прототип отличается высокой экономичностью и тяговой эффективностью. Такой двигатель уже планируют установить на сборщик космического мусора, создаваемый по программе CleanSpaceOne, а также на десятки НС, предназначенных для мониторинга радиоизлучения ультрадлинного диапазона с обратной стороны Луны (программа OLFAR).

Удалось решить и электрическое обеспечение двигательной установки при ограниченной площади солнечных батарей, питающих ионный ускоритель: один двигательный модуль с тысячевольтным инжектором и сантиметровой матрицей в 1000 микросопел потребляет в общей сложности 4 Ватта.

В отличие от традиционных ионных двигателей, обладающих значительной массой, он незначительно повлияет на массово-габаритные характеристики оснащённого им НС.

При 500 микросоплах сила такого двигателя оценивается всего в 50 мкН, однако в условиях вакуума и близкой к нулю гравитации её оказывается достаточно для корректировки орбиты НС [7].

Исходя из заявленных характеристик [6, 7], можно оценить эффективность управления НС при использовании таких миниатюрных ионных установок.

В этом случае за секунду угол поворота НС составит $\alpha_{нс} = 0{,}0005$рад, что практически совпадает с возможностями системы, использующей моментный магнитопривод.

Компактные ускорители позволят спутникам удерживать заданную орбиту, существенно продляя расчётные сроки эксплуатации.

Также двигатели малой тяги могут использоваться для управляемого схода необратимо повреждённых спутников с орбиты. Это заставит их сгорать в атмосфере Земли и частично решит проблему космического мусора. Поскольку системы ориентации на двигателях-маховиках и магнитных исполнительных органах не позволяют осуществлять изменение орбиты НС, наиболее целесообразным будет использование комбинированной системы, состоящей из магнитных катушек, позволяющих решать задачи стабилизации и ориентации, а также ионных двигателей, которые будут задействованы, в основном, для изменения орбиты НС, что позволит значительно увеличить их срок службы, а также осуществлять плановый уход с орбиты по окончании эксплуатации.

Література

1. Левантовский В. И. Механика космического полета в элементарном изложении. – М.: Наука, 1980. 512 с.
2. Суббота А. М., Симонов В. Ф., Резникова О. В. Исследование качества ориентации и стабилизации космического аппарата с использованием двигателей-маховиков и магнитных исполнительных органов // Авиационно-космическая техника и технология. – Х: ХАИ, 2013. – № 5. – С. 61-68.
3. Зараменских И.Е., Овчинников М.Ю. Расчет токовых катушек для управления макетом спутника в лабораторных условиях /Электронный ресурс/ http://www.keldysh.ru/papers/2005/prep93/prep2005_93.html
4. Бебенин Г.Г., Скреоушевский Б.С., Соколов Г.А. Системы управления полетом космических аппаратов. – М.: Машиностроение, 1978. – 176 с.
5. Урман Д. Изобретены микродвигатели для наноспутников /Электронный ресурс/ http://hi-news.ru/science/izobreteny-mikrodvigateli-dlya-nanosputnikov.html.
6. Куликов И. К Луне на одном стакане /Электронный ресурс/ http://www.gazeta.ru/science/2012/03/30_a_4111813.shtml.
7. Васильков А. Крошечный ионный двигатель будет корректировать орбиты наноспутников /Электронный ресурс/ http://www.computerra.ru/37296/37296/.

УДК 621.39

ЧАСТОТНО-ЗАГОРОДЖУВАЛЬНИЙ ФІЛЬТР 3-СМ ДІАПАЗОНУ НА ОСНОВІ МАГНІТОДІЕЛЕКТРИЧНОГО РЕЗОНАТОРА З ПРИРОДНОГО МАГНЕТИКА

Чумак Г.Л.
Київський національний університет імені Тараса Шевченка,
E-mail: Chumak_Hryhorii@mail.univ.kiev.ua

BAND-STOP filter based on magnetodielectric resonator from natural magnetic material for X-BAND

Band-stop filter based on natural mixed maghemite-hematite crystal tuned by external magnetic field is suggested and investigated. For various dielectric substrate thicknesses, maximum frequency shift of 300 MHz, Q-factor variation from 200 to 1300 and 6-20 dB rejection level is measured in 0-6 kOe field. Band-stop width at -3dB level was 8-52 MHz.

Сучасні тенденції в НВЧ техніці потребують використання нових, доступних матеріалів з магнітним впорядкуванням. В НВЧ пристроях широке застосування знайшли ферити (наприклад залізо-ітрієвий гранат). Намагнічені феритові резонатори дозволяють в одному зразку поєднати властивості діелектричного та магнітогіротропного резонатора[1]. Таким чином можна отримати високу добротність магніто-діелектричних мод з магнітною перестройкою їхніх частот В роботі пропонується загороджувальний фільтр 3 см діапазону на основі резонатора з природного магнітного матеріалу.

*Експеримент***.** Перед дослідженням НВЧ характеристик, матеріал піддавався рентгенівському фазовому аналізу, який показав наявність у матеріалі двох фаз оксидів заліза: $\gamma - Fe_2O_3$ (маґгеміт) та Fe_3O_4 (магнетит). Маґгеміт та магнетит – двохпідграткові кубічні феримагнетики зі структурою інверсної шпінелі[2].

Експериментальне дослідження проводилося на скалярному панорамному вимірювачі Р2-60 включеного за стандартною схемою на прохід. Об'єктом дослідження був макет фільтра, який представляв собою хвилевід, прямокутного перерізу $a \times b = 23 \times 10$ мм^2, з поміщеним в нього циліндричним резонатором з магнетика діаметром $d = 5,64$ мм та висотою $h = 4,27$ мм на підкладці з армованого фторопласту(АФ)(Рис.1). Зовнішнє підмагнічуюче поле величиною $H_0 = 0 - 6$ кЕ прикладалося по вісі симетрії резонатора.

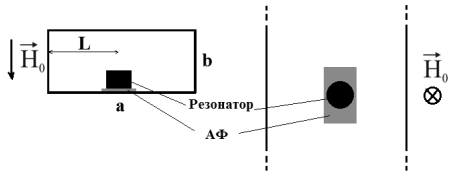


Рис.1 Геометричне положення резонатора в хвилеводі.

В ході експерименту змінювалася товщина АФ(0; 0,5; 1 мм) та геометричне розташування резонатора ($L = \frac{a}{4}; \frac{a}{2}; \frac{3a}{4}$). Вимірювалася частотна залежність коефіцієнту передачі $|S_{21}|$ резонатора при зміні величини та напрямку зовнішнього підмагнічуючого поля (Рис.2).

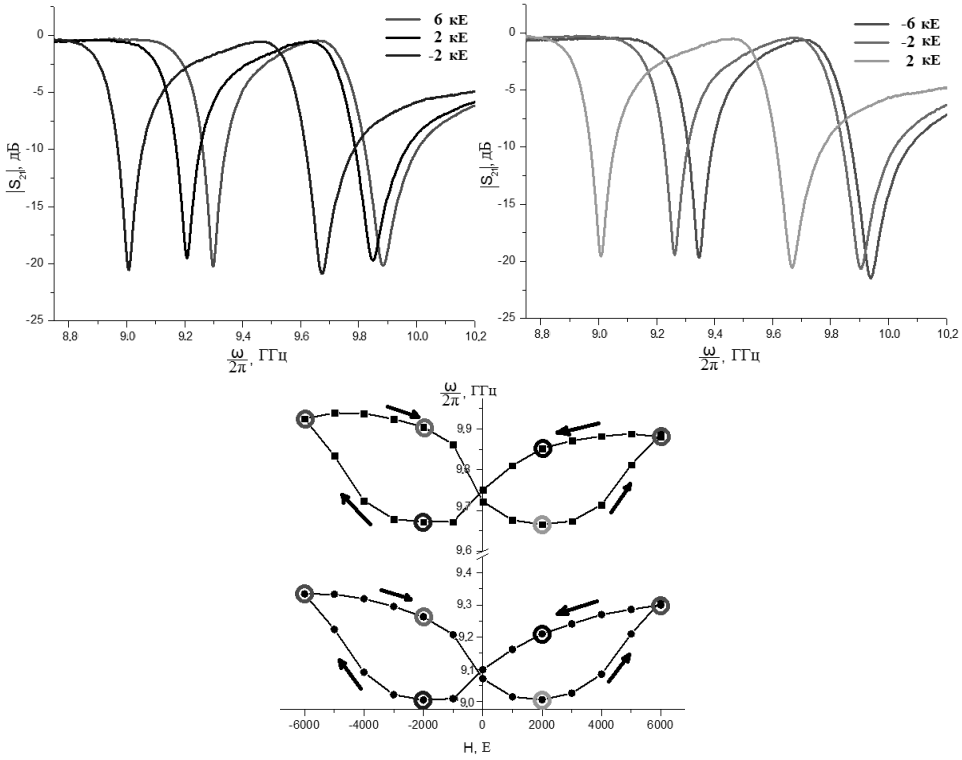


Рис. 2 Передаточні характеристики резонатора при різних значеннях зовнішнього підмагнічуючого поля (АФ – відсутній, $L = \frac{a}{2}$) та відповідні гістерезисні криві. Стрілками вказано напрямок зміни величини магнітного поля.

Таблиця 1. Результати дослідження

Товщина АФ, мм	L	$\frac{\omega_1}{2\pi}(H_0 = 0)$, *ГГц*	$\frac{\omega_2}{2\pi}(H_0 = 0)$, *ГГц*	$\Delta\frac{\omega_{1\max}}{2\pi}$, *МГц*	$\Delta\frac{\omega_{2\max}}{2\pi}$, *МГц*	Q_{01}	Q_{02}
0	$\frac{a}{2}$	9,090	9,740	300	230	340	250
0,5	$\frac{a}{2}$	10,056	10,670	40	110	670	480-630
1	$\frac{a}{4}$	10,480	10,555	84	81	550	310-460
1	$\frac{a}{2}$	10,275	10,500	50	110	580	530
	$\frac{3a}{4}$	10,500	10,575	71	74	200-880	200-1300

В таблиці 1 наведено результати для виміряних резонансних частот, максимальних перестройках резонансних частот при зміні поля в межах $H = \pm 6$ кЕ та розрахованих власних добротностях. Низькочастотна мода позначена індексом 1, високочастотна – індексом 2.

Найкраще узгодження розрахованого $|S_{21}|$ з експериментом отримано при діелектричній проникності матеріалу $\varepsilon = 20$. Використовуючи умови магнітних стінок на поверхні резонатора було розраховано частоти найнижчих власних коливань. Теоретично розрахована частота моди $E_{\pm 111}$ складає 10,5 ГГц, що з точністю 2% узгоджується з результатами отриманими для товщини АФ в 1 мм. Порушення циліндричної симетрії резонатора прямокутним хвилеводом призводить до зняття виродження по частоті мод $E_{\pm 111}$. Розподіл НВЧ полів моди E_{+111} представлено на рис. 3.

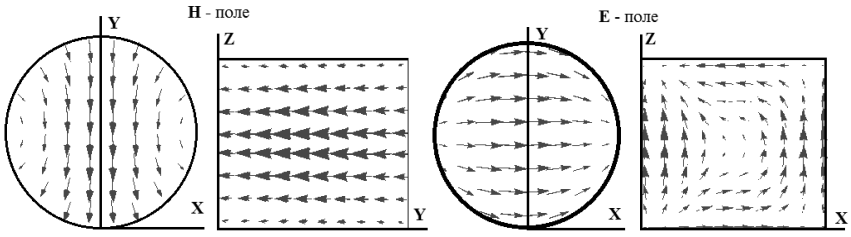


Рис.3 Розподіл електричного та магнітного поля моди E_{+111} в резонаторі.

НВЧ магнітне поле мод $E_{\pm 111}$ має радіальну та кутову компоненту, перпендикулярну до вектора намагніченості резонатора. Взаємодія мод $E_{\pm 111}$ з гіротропним магнетиком відбувається аналогічно до ефекту Коттона-Мутона. Експериментально це підтверджується незалежністю зсуву резонансних частот від напрямку намагніченості(Рис.2).

Висновки. Запропонований частотно-загороджувальний фільтр, побудований на резонаторі з природного матеріалу, дає можливість перестроювати центральну частоту в межах 3 %. Глибина загородження складає $L_0 = 6 - 20$ Дб. Позасмугові втрати становлять $1 - 6$ Дб. Ширина смуги загородження по рівню –3 Дб становить $8 - 52$ МГц. Величина власної добротності резонатора змінюється в межах від 200 до 1300. Перестройка мод $E_{\pm 111}$ резонатора має ту ж природу, що й ефект Коттона-Мутона.

Література

1. Kapilevich B.Yu. Tunable microwave ferrite filter for receiving-transmitting mobile communications systems / Kapilevich B.Yu., Safonov S.Yu. // Electromagnetic Compatibility: conf. 1990.
2. R.M. Cornell The iron oxides :Structure, properties, reactions, occurrences and uses/ R.M. Cornell, U. Schwertmann. – Weinheim: WILEY-VCH Verlag GmbH & Co.KGaA, 2003. – 667 p.

УДК 621.39

ПРЕДЕЛЬНОЕ РАЗРЕШЕНИЕ ПРОСТРАНСТВЕННЫХ СИГНАЛОВ НАВИГАЦИОННЫХ СПУТНИКОВ АЛГОРИТМА КЕЙПОНА

Шарко В. П.
ООО «Софтим», г. Киев, ул. Московская 8Е
Email: vadim.sharko@softheme.com

Capon Ultimate Resolution of Navigation Satellite Spatial Signals

The use of phase front measurements in the processing of spatiotemporal signals of global satellite navigation systems gives the possibility to determine navigation satellite's coordinates relatively to a navigation object and then determine the navigation object's coordinates. Signals of at least two navigation satellites are to be processed with the purpose of determining three coordinates and a precise time. A solution for Capon ultimate resolution of spatial signals received from two navigation satellites is investigated in this work.

Для измерения расстояний между навигационным объектом (НО) и навигационными спутниками (НС) в спутниковых навигационных системах (СНС) используются комбинации кодового и фазового псевдодальностных методов (ПМ), в основе которых лежат измерения времени распространения сигнала от НС к НО и фазы принятого сигнала относительно излучаемого [1]. Полученные значения расстояний применяются для решения системы как минимум трёх навигационных уравнений (НУ), если значение рассогласования t_{Δ} времени приёмника НО и передатчика НС равно нулю, или как минимум четырёх НУ, если $t_{\Delta} \neq 0$.

Минимальное число НУ может быть уменьшено до двух или одного при неизвестном или известном t_{Δ} соответственно, если дополнительно к временным измерениям проводятся измерения фазового фронта (ФФ) принимаемого пространственного сигнала (ПС) НС. В работе [2] предложено и проведено исследование теоретической возможности таких измерений на основе использования известных алгоритмов согласованной пространственной обработки ПС и показано, что потенциального эффективность такого подхода сравнима с эффективностью алгоритмов на основе комбинаций ПМ, используемых в СНС.

Поскольку для решения системы НУ, в которых координаты измеряются по ФФ принимаемого ПС, в общем случае требуются измерения ПС от двух НС [1], вполне очевидна необходимость исследования предельной разрешающей способности (ПРС) алгоритма обработки в зависимости от способа размещения антенных элементов (АЭ), размеров антенной системы (АС), координат НС и мощности принимаемого сигнала. Пространственная часть корреляционной

матрицы (КМ), в которую входят два входных ПС с одинаковой мощностью и некоррелированный шум, может быть представлена в виде

$$\dot{\mathbf{K}} = \left[\begin{array}{cc} \dot{\mathbf{a}}^{(1)} & \dot{\mathbf{a}}^{(2)} \end{array} \right] P \left[\begin{array}{cc} \dot{\mathbf{a}}^{(1)} & \dot{\mathbf{a}}^{(2)} \end{array} \right]^H + \mathbf{P}_0 \mathbf{I},$$

где $\dot{\mathbf{a}}^{(k)}$ - вектор-столбец k-го НС, элемент которого в случае эквидистантной антенной решётки

$$\dot{a}_i^{(k)} = U_m e^{-j\beta i b \sin\gamma_k}$$

,

$k = 1,2$ - номер НС, $i = 0 \ldots N-1$ - номер АЭ, N - число АЭ, b - шаг решётки, γ_k - угловая координата k-го НС, U_m - амплитуда ПС, $P = U_m^2$ - мощность каждого из сигналов, P_0 - спектральная плотность мощности шума в одном канале, $\mathbf{I}$ - единичная матрица. Решающая функция (РФ) $Y(\gamma)$ алгоритма Кейпона $\Upsilon(\gamma)$, записываемого в виде [3, 4]

$$\Upsilon(\gamma) = \left[\dot{\mathbf{a}}(\gamma)^H \dot{\mathbf{K}}^{-1} \dot{\mathbf{a}}(\gamma) \right]^{-1},$$

где $\dot{\mathbf{a}}(\gamma)$ - вектор-столбец опорного сигнала, элемент которого равен

$$\dot{a}_i(\gamma) = e^{-j\beta j b \sin\gamma},$$

γ - ожидаемое направление НС, получена для приведенных выше условий в виде

$$Y(\gamma) = \frac{1}{P_0} \left\{ N - \frac{q}{G^2 - H^2} \left[G \cdot \left(f_1(\gamma)^2 + f_2(\gamma)^2 \right) - 2H f_1(\gamma) f_2(\gamma) \right] \right\},$$

где $f_k(\gamma) = \sin\frac{N\varphi_k(\gamma)}{2} \Big/ \sin\frac{\varphi_k(\gamma)}{2}$, $\varphi_k(\gamma) = \varphi(\gamma) - \varphi^{(k)}$, $\varphi(\gamma) = \beta b \sin\gamma, \varphi^{(k)} = \beta b \sin\gamma_k$, $G = qN + 1$ $H = q f_{12}$, $f_{12} = \sin\frac{N\varphi_{12}}{2} \Big/ \sin\frac{\varphi_{12}}{2}$, $\varphi_{12} = \beta b \left(\sin\gamma_1 - \sin\gamma_2 \right)$, $q = P / P_0$ - отношение сигнал/шум в одном канале (ОСШ). ПРС алгоритма была найдена как значение $\Delta\gamma = \left| \gamma_1 - \gamma_2 \right|$, обращающее в ноль вторую производную РФ в точке $\gamma_{mid} = arcsin\left[\left(\sin\gamma_1 + \sin\gamma_2 \right) / 2 \right]$, т.е. как решение трансцендентного уравнения

$$\left. \frac{d^2 Y(\gamma, \Delta\gamma)}{d^2\gamma} \right|_{\gamma = \gamma_{mid}} = 0,$$

где

$$\left.\frac{d^2Y(\gamma,\Delta\gamma)}{d\gamma^2}\right|_{\gamma=\gamma_{mid}} = -\beta^2 b^2 \cos^2\gamma_{mid}\frac{qf^2}{P_0\left(G^2-H^2\right)}\times$$

$$\times\left\{N^2\cdot(G+H)ctg^2(N\phi)+2G\cdot\left[ctg^2\phi-2N\cdot ctg(N\phi)\cdot ctg(\phi)\right]+(G-H)\left(\frac{1}{\sin^2\phi}-N^2\right)\right\},$$

где обозначено $f\equiv sin(N\phi)/sin(\phi)$, $\phi=\left(sin\gamma_2-sin\gamma_1\right)/4$.

ПРС рассчитывалась для двух видов АС: «малая» АС (МАС) и «большая» АС (БАС). Число АЭ и расстояния между ними в МАС выбирались таким образом, чтобы предусмотреть возможность размещения всей АС на мобильном устройстве-коммуникаторе (например, на смартфоне с размером несколько сантиметров). Предполагалось, что БАС имеет размер несколько десятков сантиметров. Значения ПРС при неизменном ОСШ $20dB$ составили около $10..15°$ и около $1°$ для МАС и БАС соответственно. Учитывая размещение НС в орбитальной космической группировке ГЛОНАСС и GPS с минимальным угловым расстоянием между двумя соседними НС $15°..20°$ вне зависимости от орбитальной плоскости их размещения, был сделан вывод о том, что ПРС алгоритма Кейпона в применении к МАС очевидно практически недостаточна, что требует поиска других алгоритмов. В ближайшем будущем мы планируем исследование таких сверхразрешающих алгоритмов, как метод теплового шума и поиск зависимостей ПРС от степени обратной корреляционной матрицы, проекционного алгоритма, а также некоторых других.

При тех же условиях ПРС БАС имеет приемлемые значения с точки зрения различения двух любых НС.

Литература

1. Соловьёв Ю. А. Системы спутниковой навигации. – М.: Эко-Трендз, 2000. – 267 с.
2. Шарко В. П. Методика определения навигационных параметров движущихся объектов по волновому фронту сигналов радионавигационных систем: дис. на соискание науч. степени канд. техн. наук / Шарко Вадим Павлович. – Киев, 2012. – 150 с.
3. Петров В. П. Алгоритмы оценки пространственного спектра в адаптивных цифровых антенных решётках. Вестник СибГУТИ, №4, 2014. – с. 60-70.
4. Бондаренко Б. Ф., Сащук И. Н., Тимчук В. Ю. Качество обнаружения и предельное разрешение коррелированных сигналов в обнаружителях на основе алгоритма Кейпона. – Радиоэлектроника (Изв. Вузов). – К.: НТУУ «КПИ», 2004. - №7. – с. 51-60.

УДК 621.375

РОЗРОБКА КОМПЛАНАРНОГО ПІДСИЛЮВАЧА ПОТУЖНОСТІ МІЛІМЕТРОВОГО ДІАПАЗОНУ

Печора М. О., Курінний О.К., Шелковніков Б.М.
Інститут телекомунікаційних систем НТУУ «КПІ»,
ТОВ Глобал Лоджик Україна
E-mail: pechora.maksym@gmail.com

Design of complanar power amplifier for mm-wave

The article presents the result of complanar power amplifier 240 GHz based on HEMT technology simulations by using AWR packet. The results of simulation allow technological implementation of power amplifier for mm-band system.

Актуальність даної роботи обумовлена в першу чергу високою перспективністю роботи на СВЧ: ширина цього діапазон частот в 105 разів перевищує суму всіх діапазонів, використовуваних «звичайної» радіотехнікою і електротехнікою. Освоєння космічного простору, зростаюче використання електроніки НВЧ в ряді галузей народного господарства, в ракетній і атомній техніці та медицині вимагає в майбутньому ще більш широкого застосування техніки і приладів надвисоких частот [1].

Відповідно до типових показників продуктивності підсилювачів потужності (ПП) отримані змодельовані якісні показники повинні бути наступними [2]: вихідна потужність повинна бути більшою за 20 дБм, а підсилення повинно бути більшим за 20 дБ при ефективності від 30% і коефіцієнтом стійкості більшим за 1.

В даній роботі був використований в двухтактному підсилювачі потужності польовий транзистор на HEMT (High Electron Mobility transistor – транзистор з високою рухливістю електронів), тому що він має надзвичайно високі характеристики в мікрохвильовому діапазоні частот [3]. Це дозволяє отримати переваги з точки зору компктності, конкурентноспроможності, продуктивності і простоти із-за інтеграції впровадження.

Також у моделі підсилювача були використані компланарні лінії замість мікрополосків, тому що ця технологія спрощує процес виготовлення, полегшує проріджування пластини, зворотну металізацію і обробку міжшарових отворів, а також сприяє підвищеній ізоляції між сусідніми лініями і низьким характеристикам дисперсії [4].

Ця стаття представляє математичну модель та результат моделювання підсилювача потужності на частоті 240 ГГц в програмному середовищі AWR. Згідно з [5] система рівнянь в частотній області буде:

$$\frac{A_{CH}}{4}\sum_{m=-M}^{M}\sum_{n=-N}^{N}\underline{I}_{CH}^{mn}+\frac{A_C}{4}\sum_{m=-M}^{M}\sum_{n=-N}^{N}\underline{I}_{C}^{mn}+\frac{A_{Iн}}{4}\sum_{m=-M}^{M}\sum_{n=-N}^{N}\underline{I}_{H}^{mn}+\frac{A_R}{4}\sum_{m=-M}^{M}\sum_{n=-N}^{N}GA_R^t\,\underline{V}_{CH}^{mn}=$$
$$=-\frac{A_{Iвв1}}{4}\sum_{m=-M}^{M}\sum_{n=-N}^{N}\underline{I}_{вх1}^{mn}-\frac{A_{Iвв2}}{4}\sum_{m=-M}^{M}\sum_{n=-N}^{N}\underline{I}_{вх}^{mn} \quad (1)$$

де

$$\underline{I}_{c\text{н}}^{\text{mn}} = \frac{j\omega_1}{4\pi^2}\int_0^{2\pi}\int_0^{2\pi} C_H(U_{CH})W^{mn}\cdot\left[\sum_r^M\sum_s^N (r+s\frac{\omega_2}{\omega_1})\underline{U}_{CH}^{rs}W^{-r,-s}\right]\cdot d\tau_1 d\tau_2$$

$$\underline{\mathrm{I}}_{\text{н}}^{\text{mn}} = \frac{1}{\pi^2}\int_0^{2\pi}\int_0^{2\pi} \mathrm{i}_{\text{H}}\left[\sum_{\text{r}}^{\text{M}}\sum_{\text{s}}^{\text{N}} \mathrm{A}_{\text{iH}}^{\text{t}}\,\underline{\mathrm{V}}^{\text{mn}}\,\mathrm{W}^{-\text{m},-\text{n}}\right]\cdot \mathrm{W}^{\text{mn}}\mathrm{d}\tau_1\mathrm{d}\,\tau_2$$

Рис. 1 показує структурну схему підсилювача потужності на 240 ГГц, який був розроблений в середовищі AWR. При моделюванні використовувалися Т-розв'язки на вході і виході, це дозволяє підвищити вихідну потужність при порівнянні малих втратах в самій Т-розв'язці.

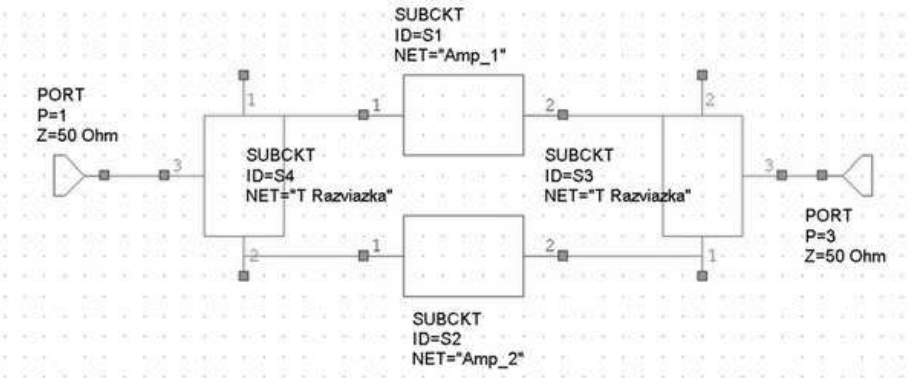


Рис. 1 Структурна схема підсилювача потужності з використанням Т-розв'язок.

Схема виконана по технології використовуватися HEMT з GaAs та компланарних ліній. Нелінійна симуляція підсилювача потужності буде реалізована методом гармонічного балансу в AWR. Цей приклад демонструє просту конфігурацію для запуску проекту підсилювача потужності. Установка має нелінійний пристрій, виконаний для дослідження потенційної продуктивністі пристрою як підсилювача потужності. Проект налаштовано для моделювання характеристик підсилювача потужності.

На рис. 2 показана повністю принципова схема двохактного підсилювача потужності.

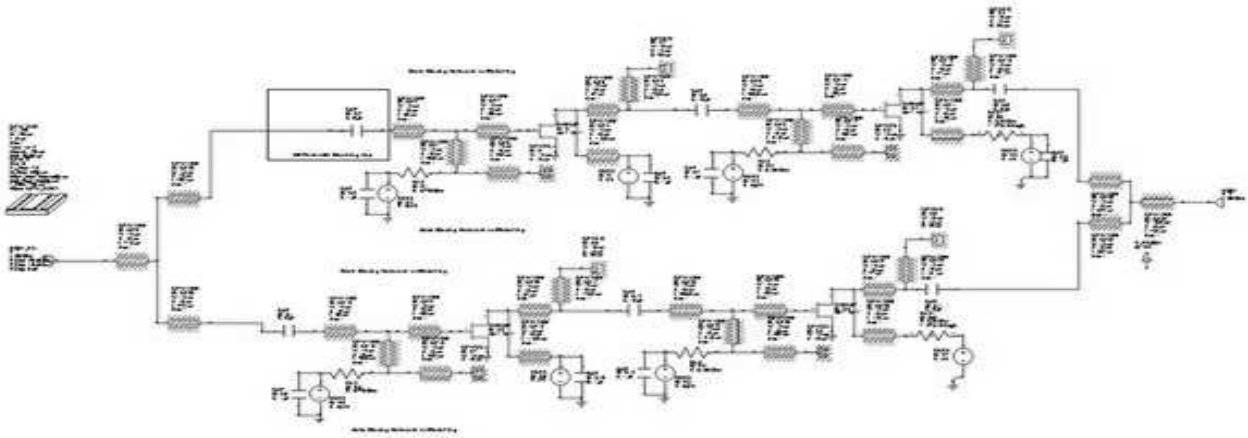


Рис. 2 Принципова схема двохтактного компланарного ПП.

Перед проведенням розрахунків були встановлені межі і крок змін напруг на електродах транзистора. Розрахунок проводився в нелінійному режимі шляхом виклику команд струм, IVCurve. Відповідна ВАХ зображена на рис. 3 разом із лінією навантаження для різної напруги зсуву.

Змодульовані S-параметри підсилювача в AWR наведено на рис. 4. Умови зміщення були V_{GS}=-0.1В, V_{DS} = 2.5 В, I_{DS} = 45 мА. Характеристики свідчать, що підсилювач має 26.91 дБ посилення в середньому і менше ніж -36 дБ вхідних втрат в діапазоні частот 230-250 ГГц.

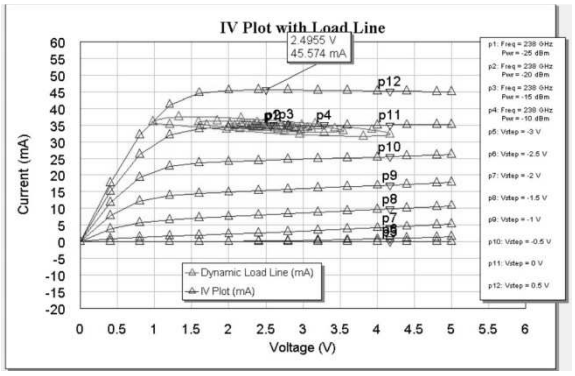


Рис.3 Сімейство вихідних статичних ВАХ польового підсилювача.

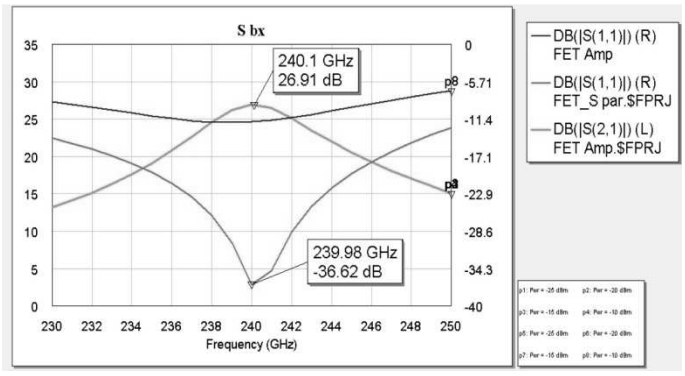


Рис. 4 Розраховані S-параметри транзистора.

Результати моделювання показують, що схема підсилювача потужності на частоті 240 ГГц з використанням HEMT і компланарних ліній задовольняє прийнятим вимогам, і на основі такого підсилювача можна приступити до проектування і технологічної реалізації, а також застосуванням в системах, які працюють в надвисоких частотах.

Література

1. Wells J. New multi-gigabit wireless systems satisfy high-security rapid response applications / J. Wells // technology Securing MIL SYSTEMS, 2006. – P. 32—34.
2. Schwoerer C. Coplanar High Performance MMICs in MHEMT and PHEMT Technology for Applicationsup to 100 GHz / C. Schwoerer, A. Tessmann, M. Leich, A. Leuther, S. Kudszus, A. Bessemoulin, M. Schlechtweg // in Proc. of GAAS, Sept. 2002.
3. Tessmann A. 220-GHz metamorphic HEMT amplifier MMICs for high- resolution imaging applications/ A. Tessmann // IEEE J. Solid-State Circuits. – 2005, Oct. – Vol. 40, No. 10. – P. 2070-2076.
4. M. Schlechtweg et al., “Coplanar Millimeter-wave IC’s for W-Band Applications Using 0.15 μm Pseudomorphic MODFETs” IEEE Journal of Solid-state Circuits, Vol. 31, n° 10, October 1996, pp. 1426-1434.
5. R. Gilmore and M. Steer, "Nonlinear circuit analysis using the method of harmonic balance -A review of the art. Part IV Introductory concepts" Int. J.Microwave Millimeter Wave Computer Aided Engineering, vol. 1, no. 1, 1991.

УДК 621.375

РАЗРАБОТКА УСИЛИТЕЛЯ МОЩНОСТИ МИЛЛИМЕТРОВОГО ДИАПАЗОНА НА ОСНОВЕ КМОП ТЕХНОЛОГИИ

Шевченко А.Л., Радченко А.А., Шелковников Б.Н.
Институт телекоммуникационных систем НТУУ «КПИ», Украина
E-mail: shevchenko.oleksandr.l@gmail.com

Development of the millimeter wave power amplifier based on CMOS technology

This paper presents the results of simulation using AWR of 140 GHz 3-stage power amplifier using CMOS technology. The results allow to procced to the next stages - development of topology, technological implementation.

В связи с растущей потребностью в передаче все больших объемов информации широкое распространение получают системы радиосвязи миллиметрового диапазона длин волн. За счет использования широкой полосы рабочих частот такие системы обеспечивают скорость передачи данных до нескольких десятков гигабит в секунду.

Для реализации современных систем радиосвязи миллиметрового диапазона длин волн необходима разработка приемопередатчиков и их составляющих элементов, выполненных в виде интегральных микросхем, что обеспечивает миниатюрность пользовательских устройств. При этом выбор технологии для реализации микросхем обуславливается в основном соображениями низкой себестоимости массового производства при обеспечении заданных технических характеристик. В связи с этим в качестве основного кандидата для создания современных СВЧ приемопередатчиков многими исследователями рассматривается стандартная КМОП технология, широко распространенная и доступная в области микроэлектроники.

В данной работе решается задача схемотехнического проектирования трехкаскадного усилителя мощности в диапазоне частот 140 ГГц, являющегося одним из основных блоков приемопередатчика миллиметровых систем связи. Усилитель мощности (УМ) в действительности является одним из главных элементов радиотракта. Разработка и моделирование блока УМ по технологии КМОП 45 нм проводились в системе автоматизированного проектирования (САПР) AWR с использованием технологической библиотеки элементов интегральных схем фабрики TSMC.

Основными характеристиками УМ являются выходная мощность и полоса рабочих частот в согласованном режиме. В результате анализа имеющихся работ [1]-[4] по исследованию усилителей мощности были сформулированы требования на характеристики разрабатываемого усилителя. К усилителю предъявлялись следующие требования: коэффициент усиления G >30 дБ; полоса пропускания 5-10 ГГц; неравномерность амплитудно-частотной характеристики (АЧХ) $\Delta G = \pm$ дБ; входной и выходной коэффициенты отражения m1 = |S11| ≤ -18 дБ, m2 = |S22| ≤ -15 дБ; выходная мощность при сжатии амплитудной характеристики на 1дБ P1dB >20 дБм; усилитель должен быть безусловно устойчивым во всем диапазоне частот, т.е. K ≥ 1, где K - инвариантный коэффициент устойчивости.

В данной работе для реализации блока УМ была выбрана схема, состоящая из трех последовательных каскадов. Схема разработанного блока УМ представлена на

Рис. 1. Основным достоинством такой архитектуры является высокий коэффициент усиления. Дополнительным преимуществом каскадной архитектуры является высокая изоляция между входом и выходом устройства, что позволило независимо разработать схемы входного и выходного согласования.

Для выполнения анализа в нелинейном моделировании используется гармонический баланс[4], который является эффективным методом для анализа усилителей мощности, смесителей, умножителей и генераторов. Моделирование с помощью гармонического баланса выполняются аналогично линейному моделированию-ввод схемы, вычисляемые в результате анализа параметры и качественные показатели. Отличие состоит в том, что для выполнения гармонического баланса требуется наличие источников напряжения, тока или мощности. Имитатор гармонического баланса позволяет определять одночастотное и многочастотное возбуждение портов, чтобы выполнить одно- и многосигнальный анализ. Всякий раз, когда источник гармонического баланса определён в схеме, имитатор гармонического баланса вызывается автоматически при моделировании. Подставим функции ряда Фурье в нелинейную математическую модель во временной области [4] и интегралы для представления комплексных амплитуд. Тогда слева и справа появится множитель $e^{j\omega kt}$, что можно сократить. Уравнения превратятся в уравнения относительно комплексных амплитуд. Для сигнала одной гармоники получим (А-матрица связей элементов и ее субматрицы):

$$A_{CH}*\sum_{k=-N(-\infty)}^{N(+\infty)}\underline{I}_{CHk}+A_C*\sum_{k=-N(-\infty)}^{N(+\infty)}\underline{I}_{Ck}+Ai*\sum_{k=-N(-\infty)}^{N(+\infty)}\underline{I}_{Hk}+A_Л*Y_Л*A^t_Л*\sum_{k=-N(-\infty)}^{N(+\infty)}\underline{V}_k=-A_{iвх}*\underline{I}_{вх},$$

где комплексные амплитуды будут иметь следующий вид:

$$V(t)=\sum_{k=-N(-\infty)}^{N(+\infty)}V_k*e^{jk\omega t}$$

$$i_{BX}(t)=\sum_{k=-N(-\infty)}^{N(+\infty)}I_{BXk}*e^{jk\omega t}$$

$$I_{Hk}=\frac{1}{2\pi}\int_{-\pi}^{\pi}i_H(A^t_{iH}*\sum_{k=-N(-\infty)}^{N(+\infty)}V_k*e^{jk\omega t})*e^{-jk\omega t}d(\omega t)$$

$$I_{Ck}=\frac{1}{2\pi}\int_{-\pi}^{\pi}C(A^t_C*\sum_{k=-N(-\infty)}^{N(+\infty)}jk\omega V_k*e^{jk\omega t})*e^{-jk\omega t}d(\omega t)$$

$$I_{CHk}=\frac{1}{2\pi}\int_{-\pi}^{\pi}C_H(\sum_{k=-N(-\infty)}^{N(+\infty)}A^t_{CH}*V_k*e^{jk\omega t})*A^t_{CH}*\sum_{k=-N(-\infty)}^{N(+\infty)}(jk\omega V_k*e^{jk\omega t})*e^{-jk\omega t}d(\omega t)$$

Система уравнений представляет собою систему операторных уравнений. Операторами в этом случае будут операторы суммы, интегральные, нелинейные. Решение. такой системы выполняется относительно комплексных амплитуд узловых потенциалов. В процессе вычисления могут быть определенные амплитуды напряжений и токов других ветвей схемы или цепи. Так как в целом мы имеем нелинейные операторы, то мы должны на конечном этапе решать систему нелинейных уравнений относительно комплексных амплитуд. Эта модель реализована средствами ПС AWR.

Схема каскада на 140 ГГц (рис.1) состоит из полевого транзистора и согласующих цепей (входного и выходного L,C фильтров, реализованных на многослойных структурах)

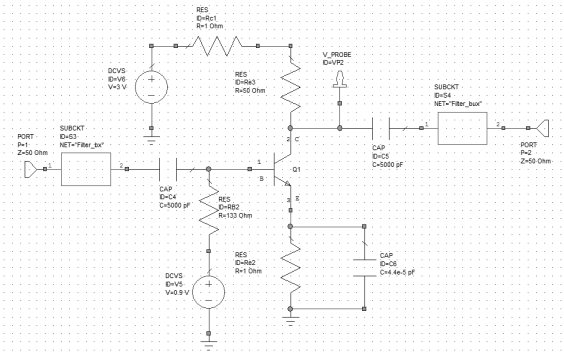


Рис. 1 Принципиальная схема одного каскада усилителя мощности.

В качестве примера результатов моделирования на рис.2-3 представлены вольт-амперная и динамическая характеристики каскада, S – параметры, показывающие коэффициент усиления, развязку и согласование. Промоделирована работа КМОП усилителя мощности, работающего на частоте 140 ГГц. Определены основные качественные показатели и характеристики. Они удовлетворяют предъявляемым требованиям от систем. Из графиков видно, что созданная модель каскада не противоречит теории радиопередающих устройств и полученные характеристики обеспечивают линейное усиления до уровня выходной мощности порядка 37 дБ в заданной полосе частот.

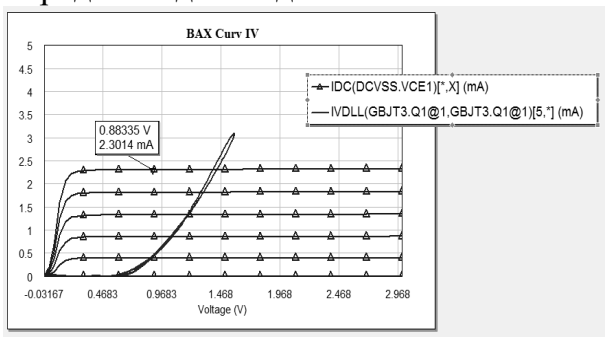


Рис. 2. Вольт-амперная и динамическая характеристики каскада

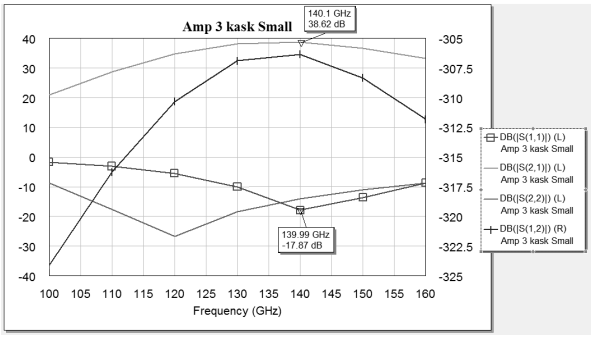


Рис.3. S – параметры, показывающие коэффициент усиления, развязку и согласование

Литература

1. Hirata Akihiko, Kosugi Toshihiko, Takahashi Hiroyuki 120-GHz-Band Millimeter-Wave Photoni Wireless Link for 10Gb/s Data Transmission // IEEE Transactions on micro-mave theory and techniquos. May 2006. Vol. 54. No. 5.
2. Wells J. New multi-gigabit wireless systems satisfy high-security rapid response applications / J. Wells // technology Securing MIL SYSTEMS, 2006. – P. 32—34.
3. B. Heydari. Millimeter Wave Devices and Circuit Blocks up to 104 GHz in 90 nm CMOS./ B. Heydari, M. Bohsali, E. Adabi, A. M. Niknejad.// IEEE JSSC, Vol. 42, No. 21, Dec. 2007, pp. 2893-2903.
4. R. Gilmore and M. Steer, "Nonlinear circuit analysis using the method of harmonic balance -A review of the art. Part IV Introductory concepts" Int. J.Microwave Millimeter Wave Computer Aided Engineering, vol. 1, no. 1, 1991.p.55.

УДК 621.39

РОЗРОБКА ЗМІШУВАЧА МІЛІМЕТРОВОГО ДІАПАЗОНУ

Курінний О.К., Печора М.О., Шелковніков Б.М.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
e-mail: kurinnyi.oleksandr@gmail.com

DESIGN OF MM-WAVE RANGE MIXER

This article presents the results of frequency mixer with range 120 GHz – 130 GHz based on HEMT technology simulations by using AWR packet. The results allow to move to the next stages -topology development and technological implementation.

Системи міліметрового діапазону, що працюють на частотах вище 100 ГГц користуються все з більшим інтересом у зв'язку з різним їх застосуванням в таких сферах, як віддалене атмосферне зондування, широкосмуговий зв'язок, та радари системи автомобільної безпеки. Понижуючі перетворювачі частот є ключовими компонентами таких систем міліметрового діапазону. Для змішувачів міліметрового діапазону існують різні технології і режими роботи. Змішувачі частот вище 100 ГГц переважно базуються на діодах Шотткі. У порівнянні з діодними, резистивні змішувачі на основі польових транзисторів мають перевагу в зниженні спотворення і низькому коефіцієнті шуму. У порівнянні з змішувачами на основі ПТ з каналом, резистивні змішувачі на основі ПТ не вимагають живлення постійного струму показують більш високу лінійність та ККД. Якісними показниками змішувача є смуга частот (сигналу, гетеродина, проміжної частоти); втрати перетворення $L_{прт}$, динамічний діапазон D; нормований коефіцієнт шуму $K_ш$; потужність гетеродина $P_г$, що відповідає мінімальним значенням $L_{прт}$ або $K_ш$. Втрати перетворення – відношення вхідної потужності сигналу до вихідної потужності на ПЧ: $L_{прт} = 10\lg(P_{НВч}/P_{ПЧ})$. Значення $L_{прт}$ залежить від якості нелінійного елемента, напруги зміщення на ньому, рівня потужності гетеродину, втрат у лініях, що підводять коливання, та їх узгодження з нелінійним елементом.

Авторами була розроблена математична модель змішувача для частотної області з двома діючими сигналами. Було застосовано метода гармонічного балансу. Виходячи з того, що якщо на нелінійний елемент з характеристикою f ($U_Н$, $I_Н$) діють сигнали двох різних частот ω_1 і ω_2, то, згідно з [5], її розкладка в ряд Фур'є буде мати вигляд:

$$f_н(t) = \frac{1}{4}\sum_{m=-M}^{M}\sum_{n=-N}^{N}\underline{\Phi}_н^{mn}\, e^{j(n\omega 1+m\omega 2)}$$

$$\underline{\Phi}_н^{mn} = \frac{1}{\pi^2}\iint_0^{2\pi} f(t)\, e^{j(m\tau 1+n\tau 2)}\, d\tau 1 d\tau 2,$$

де $\tau_1=\omega_1 t$, $\tau_2=\omega_2 t$; $\underline{\Phi}_н^{mn}$ – комплексні амплітуди гармонік.

Виразимо струм $i_{СН}$ у вигляді комплексних амплітуд, а $U_{СН}$ - у вигляді ряду Фур'є:

$$\underline{I}_{сн}^{mn} = \frac{j\omega_1}{4\pi^2}\int_0^{2\pi}\int_0^{2\pi} C_H(U_{CH})W^{mn}\cdot\left[\sum_r^M\sum_s^N (r+s\frac{\omega_2}{\omega_1})\underline{U}_{CH}^{rs}W^{-r,-s}\right]\cdot d\tau_1 d\tau_2$$

Застосуємо систему співвідношення нелінійних рівнянь для тимчасових функцій у вигляді ряду Фур'є і перейдемо в область комплексних функцій, використовуючи комплексні амплітуди та субматриці матриці зв’язку елементів А. При цьому було проведено скорочення на множник $W^{-m,-n}$. Дана система разом з рівнянням для комплексних амплітуд нелінійних компонентів являє собою систему операторних рівнянь в комплексній області. На виході отримаємо систему нелінійних рівнянь щодо комплексних амплітуд $\underline{V}$,$\underline{U}$:

$$\underline{I}_{н}^{mn} = \frac{1}{\pi^2}\int_0^{2\pi}\int_0^{2\pi} i_H\left[\sum_r^M\sum_s^N A_{iH}^t\,\underline{V}^{mn}\,W^{-m,-n}\right]\cdot W^{mn}d\tau_1 d\,\tau_2\,,$$

$$\underline{I}_{сн}^{mn} = \frac{j\omega_1}{4\pi^2}\int_0^{2\pi}\int_0^{2\pi} C_H(U_{CH})W^{mn}\cdot\left[\sum_r^M\sum_s^N (r+s\frac{\omega_2}{\omega_1})\underline{U}_{CH}^{rs}W^{-r,-s}\right]\cdot d\tau_1 d\tau_2$$

$$\frac{A_{CH}}{4}\sum_{m=-M}^{M}\sum_{n=-N}^{N}\underline{I}_{CH}^{mn}+\frac{A_C}{4}\sum_{m=-M}^{M}\sum_{n=-N}^{N}\underline{I}_{C}^{mn}+\frac{A_{Iн}}{4}\sum_{m=-M}^{M}\sum_{n=-N}^{N}\underline{I}_{H}^{mn}+\frac{A_R}{4}\sum_{m=-M}^{M}\sum_{n=-N}^{N}GA_R^t\,\underline{V}_{CH}^{mn}=$$

$$=-\frac{A_{Iвв\,1}}{4}\sum_{m=-M}^{M}\sum_{n=-N}^{N}\underline{I}_{вх\,1}^{mn}-\frac{A_{Iвв\,2}}{4}\sum_{m=-M}^{M}\sum_{n=-N}^{N}\underline{I}_{вх}^{mn}$$

Ця стаття представляє результати моделювання змішувача діапазону частоти 120 ГГц - 130 ГГц в ПС AWR. Польові транзистори виконані за технологією GaAs mHEMT 0.06-0,1 мкм з типовими параметрами (Gm) max = 1400 mS / mm, (ID) max = 900 mA / mm і ft і Fmax 200 ГГц і 300 ГГц відповідно.

Модель змішувача на польовому транзисторі з подвійним затвором (складений транзистор) було реалізовано в ПЗ AWR на концентрованих елементах. Принципова схема даного змішувача показана на рис. 1.

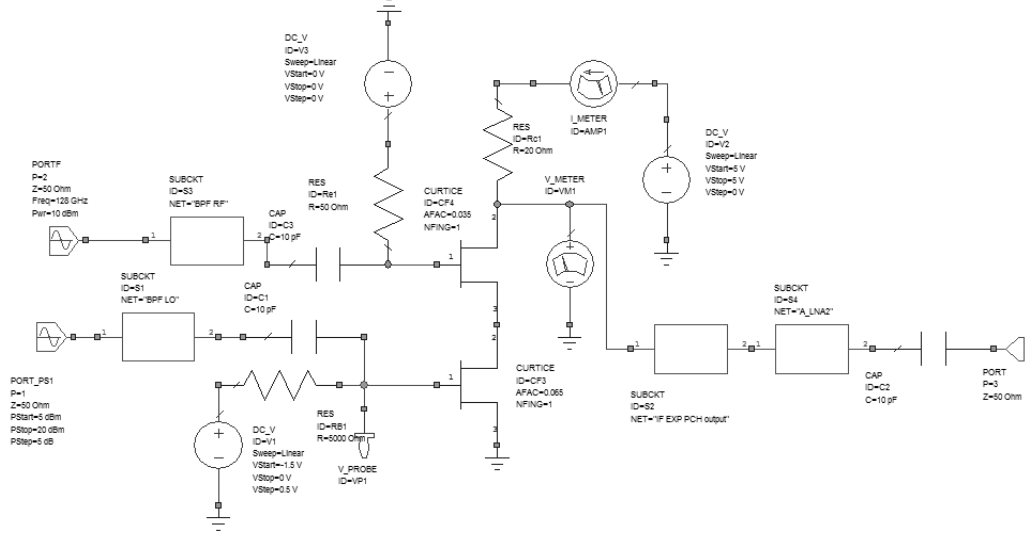


Рис. 1 Принципова схема змішувача на ПТ з подвійним затвором.

В процесі моделювання важливим етапом є визначення режиму роботи транзистора. За допомогою динамічних кривих та статичних ВАХ визначаємо робочу точку. З рис. 2 робоча точка має параметри: U_{CH} = 1,5 В; i_{CH} = 0,031 мА.

Важливою складовою змішувача є фільтри, відповідно каналів РЧ, гетеродину та ПЧ. Крім придушення побічних частотних продуктів вони виконують функцію узгодження. Фільтри виконані на мікрополоскових лініях. S-параметри фільтрів продемонстровані на рис. 3. З графіку видно, що відбувається

ослаблення відбитої хвилі в каналі гетеродина на 38 Дб (частота 130ГГц) та в РЧ каналі на 35,5 Дб (частота 120ГГц).

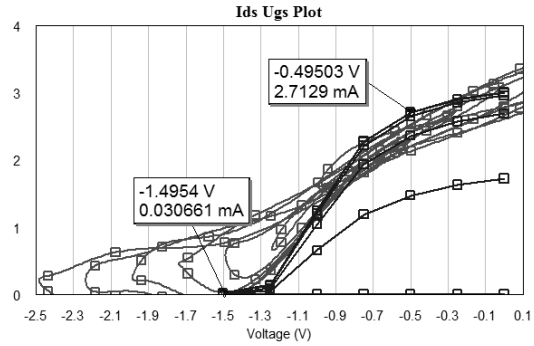


Рис. 2 Графік вхідних характеристик - динамічних кривих та сімейства статичних ВАХ

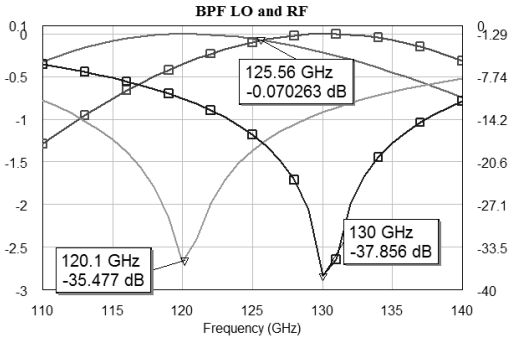


Рис. 3 Характеристики фільтрів та коефіцієнт передачі в каналах гетеродина та радіочастоти

Для забезпечення необхідного коефіцієнта передачі, на виході змішувача встановлено малошумний підсилювач потужності. Його характеристики представлені на рис. 4.

Одним з важливих параметрів роботи змішувача є потужність на виході, тобто сигналу проміжної частоти. На рис. 5 показано спектральну потужність для сигналу частотою 2 ГГц (ослаблення 20 мДб).

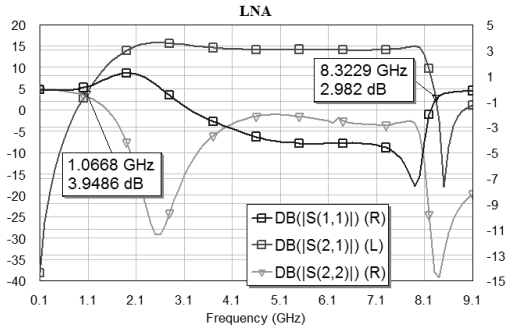


Рис. 4 S-параметри вихідного малошумного підсилювача

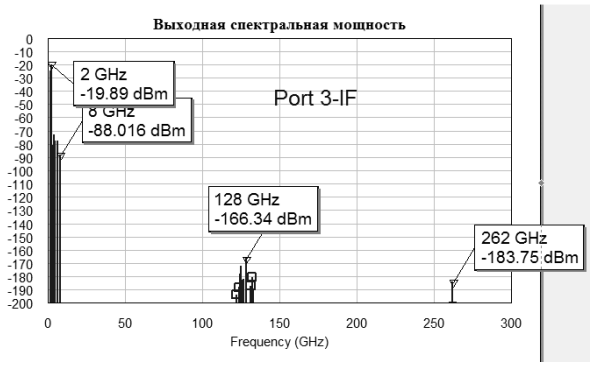


Рис. 5 Графік спектральної потужності на виході змішувача

В роботі було реалізовано активний субгармонічний змішувач на подвійному ПТ за технологією 50 нм mHEMT. Серед переваг - менший коефіцієнт шуму, нижчі вимоги до живлення гетеродину (LO), частотний діапазон роботи змішувача. Метаморфічна HEMT технологія продемонструвала потенціал для подальшого розвитку систем міліметрового та суб-міліметрового діапазону, що використовуються, зокрема, в космічних апаратах.

Література

1. A. Hülsmann, A. Leuther, I. Kallfass & others, “Advanced mHEMT technologies for space applications”// 20th International Symposium on Space Teraherz Technology, April 2009
2. I. Kallfass, “Active Integrated Circuits in Millimeterwave Applications Summer Term 2011”// Lecture Part 4 Nonlinear Circuits V: Frequency Mixers
3. Leuther, A. Tessmann & others, “35 nm Metamorphic HEMT MMICTechnology,” 20th International Conference on Indium Phosphide and Related Materials, MoA3.3, May 2008.
4. R. Gilmore and M. Steer, "Nonlinear circuit analysis using the method of harmonic balance -A review of the art. Part IV Introductory concepts" Int. J.Microwave Millimeter Wave Computer Aided Engineering, vol. 1, no. 1, 1991.

УДК 621.382

РАЗРАБОТКА МАЛОШУМЯЩЕГО УСИЛИТЕЛЯ МИЛЛИМЕТРОВОГО ДИАПАЗОНА

Радченко А.А, Шевченко О.Л., Шелковніков Б.М.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail:murano500k@gmail.com

Design low-noise amplifier for mm-wave

This article presents the results of 120 GHz low noise amplifier based on SiGe simulations by using AWR packet. The results allow to use model in the next stage: topology development and technological implementation

Интерес к системам, работающих на частотах выше 100 ГГц непрерывно растет. Применение варьируются от атмосферной радиометрии до автомобильных, радиолокационных, сенсорных и телекоммуникационных систем[1-4]. В следствии большого затухания мм волн в атмосфере, основной задачей для систем, работающих в данном диапазоне частот, является использование приемника с высокой чувствительностью с надлежащим усилением, что позволяет сократить энергопотребление системы. Поэтому разработка малошумящих усилителей(МШУ) для систем, работающих на частотах выше 100 ГГц является актуальной.

Эта статья представляет математическую модель и результаты моделирования малошумящего усилителя 120 ГГц в AWR MWO. Перед началом моделирования были составлены требования к качественным показателям МШУ: центральная частота усиления f = 120ГГц, коэффициент усиления больше 5 дБ. коэффициент шуму в полосе рабочих частот менее 4 дБ; значения входного и выходного коэффициентов отражения не более -30 дБ, напряжение питания менее 1.5 В, волновые сопротивления входного и выходного каскадов 50 Ом, усилитель должен быть безусловно устойчивым на рабочем диапазоне (k> 1).

Схема выполнена по технологии SiGe FET 0.06-0,1 мкм. В качестве основного элемента выбрана модель биполярного транзистора CURTICE Nonlinear FET model из пакета AWR. Инженерный метод моделирования СВЧ транзисторов, позволяет достаточно быстро получить структурную модель проектируемого прибора на основе бесструктурных моделей серийных транзисторов

Теоретической основой моделирования усилителей является метод гармонического баланса и аппарат S-матриц. Метод гармонического баланса (МГБ) позволяет получить качественные показатели на основе нелинейного анализа (при большом сигнале) а аппарат S-матриц позволяет получить результаты в линейном представлении.

Согласно МГБ [5] система уравнений в частотной области будет:

$$\frac{A_{CH}}{4}\sum_{n=-N}^{N} I_{CH}^{n} + \frac{A_{C}}{4}\sum_{n=-N}^{N} I_{C}^{n} + \frac{A_{Iн}}{4}\sum_{n=-N}^{N} I_{H}^{n} + \frac{A_{R}}{4}\sum_{n=-N}^{N} GA_{R}^{t}\,\underline{V}_{CH}^{n} =$$

$$= -\frac{A_{Iвв\,1}}{4}\sum_{n=-N}^{N} I_{вх\,1}^{n} - \frac{A_{Iвв\,2}}{4}\sum_{n=-N}^{N} I_{вх\,2}^{n}$$

где:

$$I_{сн}^{n} = \frac{j\omega_1}{4\pi^2}\int_{0}^{2\pi} C_H(U_{CH})W^{n}\cdot\left[\sum_{s}^{N}(r+s\frac{\omega_2}{\omega_1})\underline{U}_{CH}^{rs}W^{-r,-s}\right]\cdot d\tau_1 d\tau_2$$

$$I_{н}^{n} = \frac{1}{\pi^{2}} \int_{0}^{2\pi} i_{н} \left[\sum_{s}^{N} A_{iH}^{t} \underline{V}^{n} W^{-n} \right] \cdot W^{n} d\tau_{1} d\tau_{2}$$

Эта система реализована на элементной базе AWR. Структурная схема однокаскадного МШУ, которая была разработана в среде AWR, состоит из согласующей цепи на входе, полевого транзистора и согласующей цепи на 120 ГГЦ.

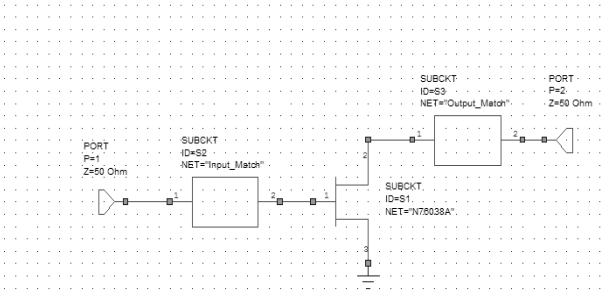


Рис. 1. Структурная схема одного каскада МШП.

В процессе моделирования были согласованы входная и выходная цепь усилителя, реализованные на копланарах, выбрана рабочая точка и оптимизированы токи и напряжения, подаваемые на транзистор, также были рассчитаны основные характеристики усилителя. Графики коэффициентов передачи и отражения усилителя показаны на рис. 2 и рис. 3. Также была исследована стабильность работы прибора в заданном диапазоне частот (рис. 4). В заданной полосе частот коэффициент усиления мощности 1.6 дБ, коэффициент шума меньше 4.5 дБ. Значения коэффициента стабильности больше 1 на всей полосе частот, при 120 ГГц равно 1.28. Результаты моделирования показали, что однокаскадный МШУ не дает достаточного коэффициента усиления, поэтому было решено смоделировать усилитель с двумя каскадами. При применении 2-х каскадов характеристики усилителя значительно улучшились. Как можно увидеть на рис. 4 и рис. 5, усиление удалось увеличить до 5.1 дБ, что удовлетворяет предъявленные требования. Также были получены кривые ВАХ транзистора на уровнях от -0.5 до 3 В (рис. 6) и график выходной мощности двух каскадов МШУ (рис. 7).

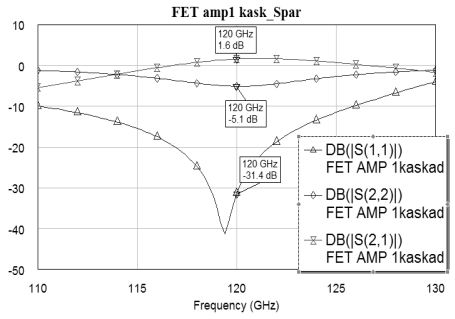


Рис. 2 Значение коэффициентов отражения и передачи однокаскадного усилителя в частотной области

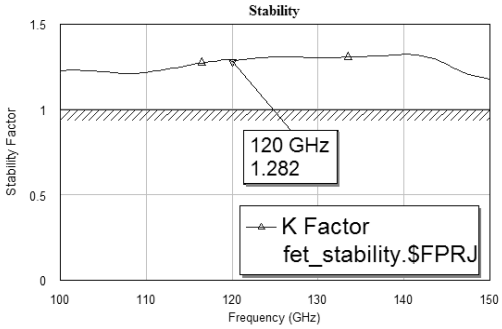


Рис. 3 График измерения стабильности транзистора

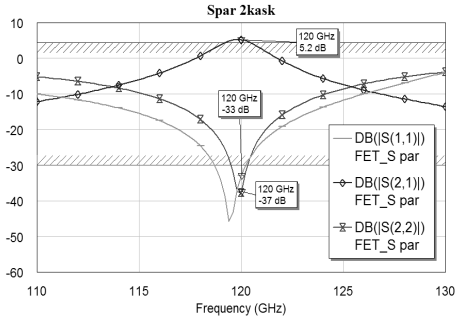


Рис. 4 Значение коэффициентов отражения и передачи двух каскадов в частотной области

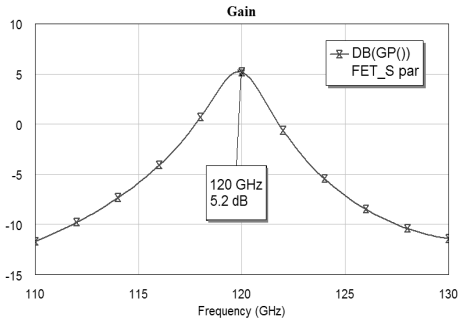


Рис.5 График усиления 2-х каскадного МШУ

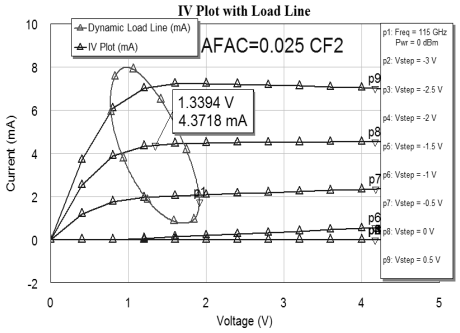


Рис. 6 Семейство выходных статических ВАХ биполярного транзистора. (Верхняя кривая соответствует напряжению на затворе транзистора Uз0= 0.5 В, нижняя - напряжению Uз0= -3 В)

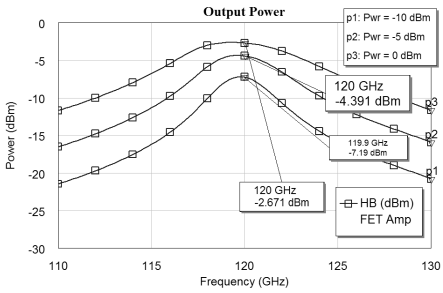


Рис. 7 Значения выходной мощности двух каскадного МШУ при -10, -5, 0 дБм на входе

Промоделирована работа малошумящего усилителя SiGe на 120 ГГц. Определены основные качественные показатели и характеристики. Они удовлетворяют заданным требованиям.

Литература

1. Wells J. New multi-gigabit wireless systems satisfy high-security rapid response applications / J. Wells // technology Securing MIL SYSTEMS, 2006. – P. 32—34.
2. Schwoerer C. Coplanar High Performance MMICs in MHEMT and PHEMT Technology for Applicationsup to 100 GHz / C. Schwoerer, A. Tessmann, M. Leich, A. Leuther, S. Kudszus, A. Bessemoulin, M. Schlechtweg // in Proc. of GAAS, Sept. 2002.
3. Tessmann A. 220-GHz metamorphic HEMT amplifier MMICs for high- resolution imaging applications/ A. Tessmann // IEEE J. Solid-State Circuits. – 2005, Oct. – Vol. 40, No. 10. – P. 2070-2076.
4. M. Schlechtweg et al., “Coplanar Millimeter-wave IC’s for W-Band Applications Using 0.15 μm Pseudomorphic MODFETs” IEEE Journal of Solid-state Circuits, Vol. 31, n° 10, October 1996, pp. 1426-1434.
5. R. Gilmore and M. Steer, "Nonlinear circuit analysis using the method of harmonic balance -A review of the art. Part IV Introductory concepts" Int. J.Microwave Millimeter Wave Computer Aided Engineering, vol. 1, no. 1, 1991.

УДК 621.391

МОДИФІКАЦІЯ АЛГОРИТМУ КЕЙПОНА ДЛЯ ВИЗНАЧЕННЯ ПЕЛЕНГУ НА ДЖЕРЕЛА РАДІОВИПРОМІНЮВАННЯ ПРИ СФЕРИЧНИХ ФРОНТАХ ЇХ ЕЛЕКТРОМАГНІТНИХ ХВИЛЬ У МІСЦІ ПРИЙОМУ

Авдєєнко Г.Л., Корсак В.В., Якорнов Є.А.
Інститут телекомунікаційних систем НТУУ «КПІ»
E-mail:yakornov@its.kpi.ua

Capon's algorithm modification for radiation source with spherical waves bearing angle estimation

Capon's algorithm of radiation source bearing angle estimation limitations are shown when radiation source located in the Fresnel's zone of the direction-finder antenna system. Modification of Capon's algorithm in order to determine bearing angle and distance to raditation source with spherical wave front from direction-finder antenna system are proposed.

Алгоритм Кейпона є одним з відомих алгоритмів пеленгації джерел радіовипромінювання (ДРВ) високої роздільної здатності [1]. Даний алгоритм передбачає обчислення функції вихідних сигналів лінійної антенної решітки (АР), на яку приходить електромагнітна хвиля (ЕМХ) з плоским фазовим фронтом (рис.1) і, зокрема, визначення пеленгу до джерела радіовипромінювання (ДРВ) за допомогою наступного базового співвідношення

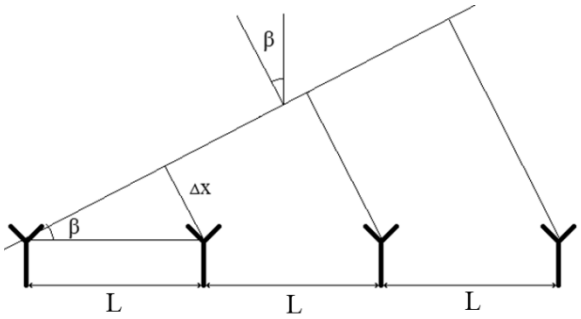


Рис.1 Лінійна АР та плоский фронт хвилі

$$V(\beta)=\frac{1}{F^2(\beta)\cdot \mathbf{S}_{\alpha}^{\mathbf{H}}(\beta)\cdot \mathbf{R}_{\mathbf{xx}}^{-1}(\beta)\cdot \mathbf{S}_{\alpha}(\beta)}\ , \qquad (1)$$

де $F(\beta)$ – діаграма спрямованості окремого елементу АР (вважатимемо всі елементи АР ідентичними); $\mathbf{R}_{\mathbf{xx}}=E\left[\mathbf{x}(t)\cdot\mathbf{x}^{H}(t)\right]$ – коре-ляційна матриця вхідних сигналів антенної решітки, які усереднені в часі; $\mathbf{x}(t)=\left[x_1(t)\ \ x_2(t)\cdots x_N(t)\right]^{\mathrm{H}}$ – вектор-стовпець вхідних сигналів антенної решітки; $\mathbf{S}\alpha(\beta)$ – управляючий вектор-стовбець антенної решітки; N – кількість елементів АР.

З урахуванням того, що Δx з рис.1 і набіги фаз, за рахунок різної відстані кожного елементу решітки до ДРВ будуть рівні

$\Delta x = L\sin\beta \ \Rightarrow\ t_1=\frac{\Delta x}{c}=\frac{L}{c}\sin\beta=\Delta\varphi$, то вектор $\mathbf{S}\alpha(\beta)$ можна представити в вигляді

$$\mathbf{S}_{\alpha}(\beta)=\begin{bmatrix}1\\ \exp(-j(2\pi L\sin\beta)/\lambda)\\ \vdots\\ \exp(-j((N-1)\pi L\sin\beta)/\lambda)\end{bmatrix} \tag{2}$$

Як можна побачити з виразу (2) для плоского фазового фронту ЕМХ, управляючий вектор-стовбець $\mathbf{S\alpha}(\beta)$ функціонально залежить лише від кута приходу (пеленгу) ЕМХ β, а отже функція вихідних сигналів лінійної антенної решітки V(β) також залежить лише від цього кута. Відповідно, побудувавши залежність V(β), можливо по її максимумам отримати інформацію лише про пеленг до ДРВ.

Однак, для ряду практичних застосувань, коли ДРВ знаходиться в зоні Френеля, фронт ЕМХ сферичний (рис.2) і визначення пеленга за допомогою виразу (1) призводить до великих помилок.

У роботах [2,3] для цієї зони при визначенні пеленга запропоновано використовувати фазові зрушення щодо центральної антени і показано, що сферичність фронту ЕМХ дозволяє додатково визначати дальність до ДРВ. Однак реалізація цих систем вимагає застосування точних і дорогих фазометрів, що стримує їх впровадження. Тому проаналізуємо можливість роботи алгоритму Кейпона для зони Френеля АР пеленгатора. Для сферичного фронту ЕМХ набіги фаз між і-им та центральним елементом АР можна визначити як

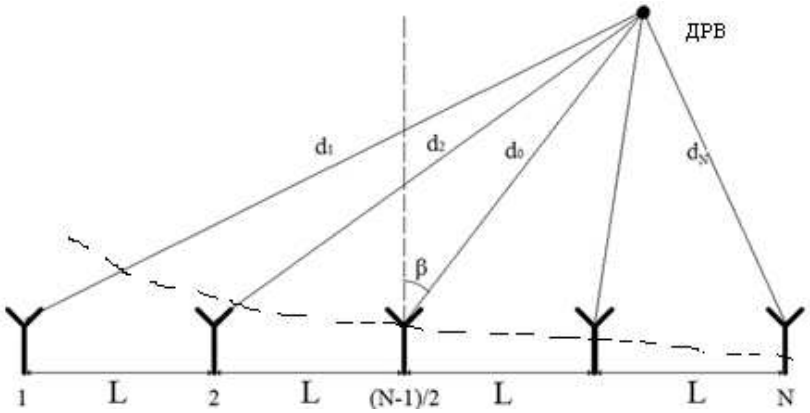


Рис. 2 Лінійна АР та сферичний фронт хвилі

$$\varphi_i=\frac{2\pi}{\lambda}(d_i-d_0),\ i=\overline{1,N} \tag{3}$$

де d_i – відстань від і-го елементу АР до ДРВ, яка згідно з рис.2, дорівнює

$$d_i=d_i(\beta,d_0)=\sqrt{\left(\frac{L(N-1)}{2}\right)^2+d_0^2-2d_0\left(\frac{L(N-1)}{2}\right)\cos(90^\circ+\beta)}\ . \tag{4}$$

Управляючий вектор-стовпець АР можна подати у вигляді

$$\mathbf{S}_{\alpha}(\beta_0,d_0)=\begin{bmatrix}1\\ \exp(-jkd_1(\beta,d_0))\\ \vdots\\ \exp(-jkd_N(\beta,d_0))\end{bmatrix}. \tag{5}$$

Як наслідок, модифікований алгоритм Кейпона передбачає обчислення функції вихідних сигналів лінійної АР, яка залежить як від кута приходу β, так і від дальності

$$\mathrm{V}(\beta,d_0)=\frac{1}{F^2(\beta)\cdot\mathbf{S}_{\alpha}^{\mathbf{H}}(\beta,d_0)\cdot\mathbf{R}_{\mathbf{xx}}^{-1}(\beta)\cdot\mathbf{S}_{\alpha}(\beta,d_0)} \tag{6}$$

Отже, визначивши управляючий вектор для сферичного хвильового фронту, що дозволяє враховувати кривизну фронту ДРВ, при заданій геометричній конфігурації АР, алгоритм визначення кута і відстані до ДРВ, розташованих в ближній зоні (БЗ) і зоні Френеля АР пеленгатора можна представити такими кроками:

1) визначення кількості джерел в дальній зоні (ДЗ) по максимуму функції (1) вихідних сигналів *VД.З.*(*β*);

2) обчислення функції *V*(*β,d*) в декількох точках БЗ на фіксованих дальностях *dk: d1=RД.З., d2=0,75RД.З., d3=0,5RД.З., d4=0,25RД.З., d5=0,125RД.З.* і.т.д., де *RД.З.* – границя ДЗ;

3) визначення з отриманої сукупності дальностей в БЗ (*d1,…dk*) тієї пари суміжних значень (*di,di+1*), які описують діапазон дальностей *Δd=di-di+1*, при яких спостерігаються максимальні «сплески» функції *V*(*β,d*) згідно (6), тобто конкретизація тієї частини зони, в яких знаходяться ДРВ;

4) розбиття діапазону *Δd* на піддіапазони з кроком *δd* (*Δd=Nδd* (див.рис.3) і обчислення функції *V*(*β,d*) (рис.4) в точках *dn=di+nδd*, *n* = 1…К.

5) визначення за отриманою сукупністю (*V*(*β1,d1*)… *V*(*βn,dn*)) шуканої дальності *d* і пеленга *β* ДРВ за правилом (*d,β*)=argmax(*V*(*βi,di*)), *i* = 1…К, причому оцінка дальності буде тим точніша, чим менший крок *δd*.

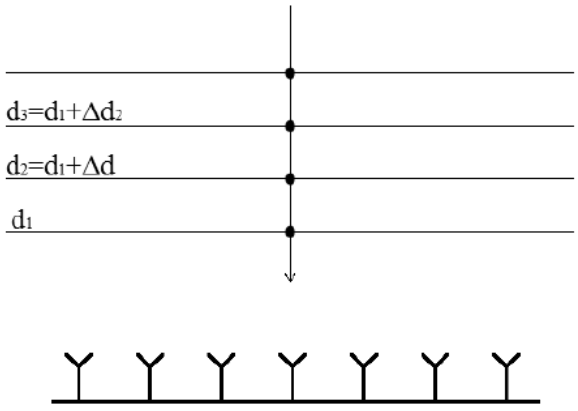


Рис. 3 Лінійна АР та відстань, на яку вона фокусується

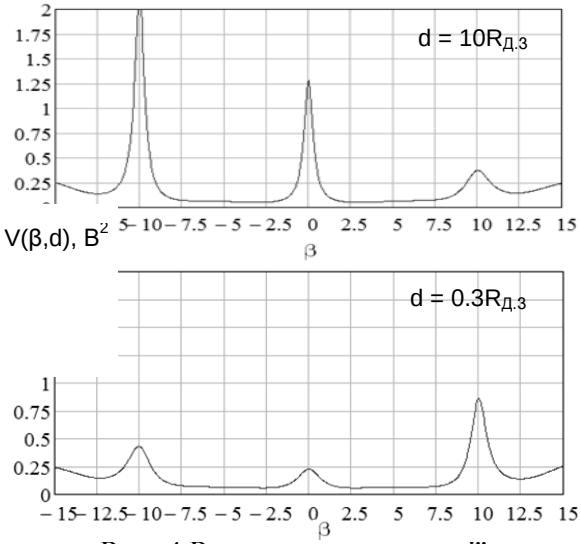


Рис. 4 Результати пеленгації по модифікованому алгоритму Кейпона

У доповіді також представлені деякі результати моделювання по даному алгоритму.

Література

1. J. Capon. High-Resolution Frequency-Wavenumber Spectrum Analysis. Proc. IEEE, Vol. 57, No. 8, August 1969.
2. Авдеенко Г.Л., Федоров В.И., Якорнов Е.А. Определение местоположения источника радиоизлучения по кривизне фронта электромагнитной волны. Известия вузов. Радиоэлектроника. - 2008. № 3. – с. 3-11.
3. Авдеенко Г.Л., Липчевская И.Л., Якорнов Е.А. Фазовые системы определения координат источника радиоизлучения гармонического сигнала в зоне Френеля. Известия ВУЗов. Радиоэлектроника. 2012. № 2. – с. 24-33.

УДК 621.391

МОНІТОРИНГ РАДІОВИПРОМІНЮВАННЯ В БЛИЖНІЙ І ПРОМІЖНІЙ ЗОНАХ НА ОСНОВІ АЛГОРИТМУ КЕЙПОНА

Авдєєнко Г.Л., Корсак В.В., Якорнов Є.А.
Інститут телекомунікаційних систем НТУУ «КПІ»
E-mail:yakornov@its.kpi.ua

Radio emission monitoring with Capon's algorithm usage in the near and intermediate zones

Spatial selection of radio emission source in near and intermediate zone with modified Capon's algorithm usage in direction-finder of the frequency monitoring system is presented. It is shown that 10.5 GHz interference suppression during intermediate zone's signal-of-interest selection from interferences with almost same bearing angle is not less than 16 dB.

Сучасні системи моніторингу радіовипромінювання (СМРВ) мають виконувати такі функції [1]:

- надання адміністрації, що керує використанням електромагнітного спектра, інформації про фактичне використання частот;
- вимірювання технічних параметрів випромінювань радіоелектронних засобів (РЕЗ) і високочастотних пристроїв, перевірка їх відповідності регламентам, сертифікатам і ліцензіям;
- рішення оперативних, планових та фонових задач радіоконтролю; виявлення, ідентифікація і локалізація на місцевості несанкціонованих джерел радіовипромінювання (ДРВ) і джерел радіозавад, а також джерел, заборонених до експлуатації;
- дослідження в галузі розповсюдження радіохвиль і електромагнітної сумісності РЕЗ для вдосконалення методів планування використання спектра.

Зокрема, мобільна станція [1] здатна виконувати завдання радіоконтролю, в тому числі і сигналів цифрових мереж зв'язку GSM, UMTS, CDMA, TETRA, DECT, а також Wi-Fi і WiMAX та сигналів цифрового телебачення DVB-T/T2 при умові, що джерела находяться в дальній зоні (ДЗ). Однак методи пеленгування, закладені в таких системах, не можуть розділити сигнал від завади у випадку, коли джерела їх випромінювання знаходяться на одному пеленгу по відношенню до системи моніторингу.

Розглянемо можливість розділення сигналів на одному пеленгу на основі модифікованого для ближньої і проміжної зон (БЗ) алгоритму Кейпона [2], який використовує відмінності в сферичності фронтів їх електромагнітних хвиль (ЕМХ).

Для цього визначимо наступну послідовність кроків вирішення задачі:

1) сканування простору, обмеженого певним кутом, для того щоб отримати значення пеленгів, з яких приходять сигнали від різних ДРВ;

2) застосування модифікованого алгоритму Кейпона [2], що враховує кривизну фазового фронту і визначення відстані до кожного з ДРВ;

3) розрахунок згідно [2] адаптивним процесором кореляційної матриці адитивної суміші всіх вхідних сигналів $\mathbf{R}_{xx}$, оберненої кореляційної матрицю вхідних сигналів $\mathbf{R}_{xx}^{-1}$ та обчислення вектора-стовпця S_α просторової структури сигналу цього джерела на розкриві АР;

4) розрахунок вектору вагового коефіцієнту АР за критерієм середньоквадратичного відхилення;

5) перемноження вирішуючим пристроєм адитивної суміші сигналів в кожному каналі АР СМРВ на відповідний ваговий коефіцієнт (шляхом вибору необхідного зсуву фаз та внесеного ослаблення амплітуди сигналів) і складання цих перемножених сигналів формування діаграми спрямованості (ДС), яка селектує досліджуваний сигнал від інших завадових. Для виділення кожного з сигналів необхідно сформувати різні вагові коефіцієнти і відповідно різні ДС;

6) після завершення селекції ДРВ можна досліджувати параметри кожного із сигналів окремо від інших.

Один з варіантів спрощеної схемної реалізації підсистеми просторової обробки СМРВ по даному алгоритму наведено на рис. 1.

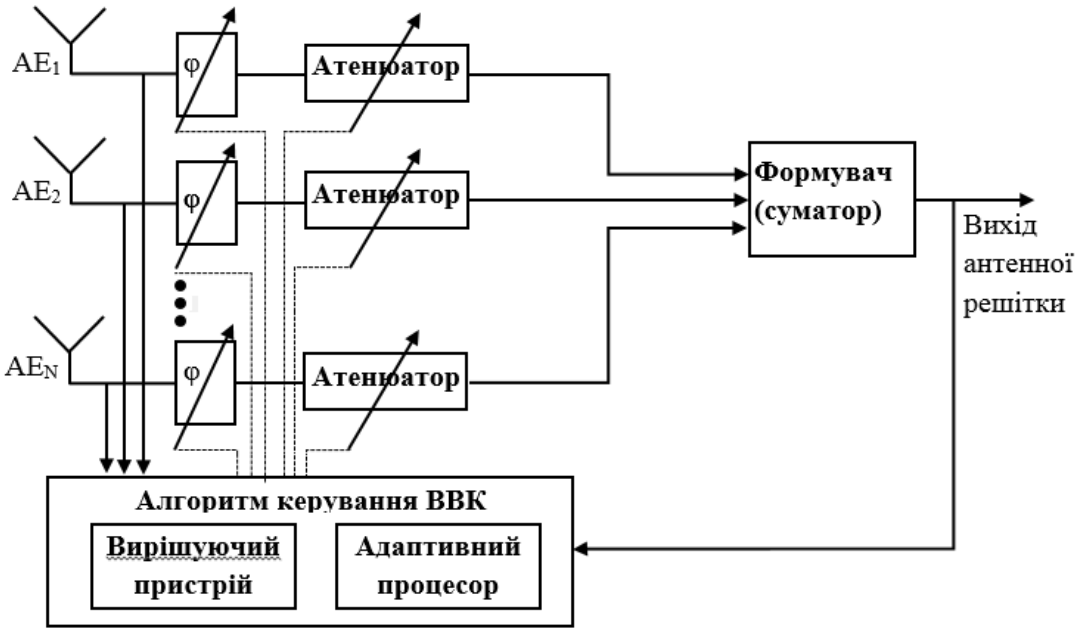


Рис. 1 Підсистема просторової обробки сигналів СМРВ.

Перевірка працездатності запропонованого алгоритму здійснювалася в програмному середовищі Mathcad для наступних вихідних даних: несуча частота f=10,5 ГГц, кількість елементів АР M=10, ширина бази L=2λ = 6 см, ширина спектра корисного сигналу Δf =8 МГц, інтервал дискретизації (для всіх сигналів) Δt=1/2Δf = 62.5 нс, час спостереження T=10 мс, число дискрет на інтервалі спостереження N=160, ширина діаграми спрямованості (ДС) елементу АР по нулях $2\theta_0 = 44^0$. Для цих даних згідно з першим кроком алгоритму напрямки пеленгів по функції Кейпона для плоского фронту ЕМХ зображені на рис. 2. Після того як пеленг завади буде визначений, вирішуючий пристрій вираховує за рівнянням Вінера-Хопфа вагові

коефіцієнти для того, щоб сформувати провали в ДС в кутових напрямках, звідки приходить завада.

Для пеленгації ДРВ зі сферичним фронтом ЕМХ скористаємося модифікованим алгоритмом Кейпона [2].

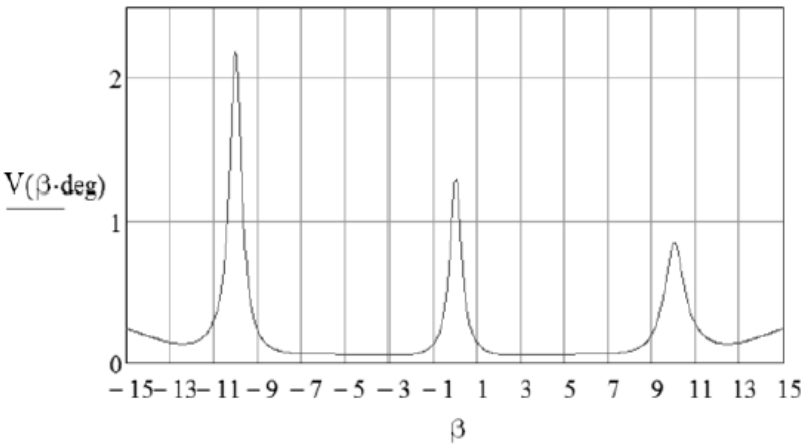


Рис.2 Кутовий спектр напрямів надходження сигналів.

Моделювання просторової селекції сигналів для кутових положень пеленгів, зображених на рис. 2, показало добрі результаті по придушенню завади у БЗ. Так, наприклад, після просторової селекції корисного сигналу, що розташовувався на нульовому пеленгу в ДЗ, його рівень підсилився на 5,8 дБ, сигнал першої завади, яка також розташовувалася в ДЗ, але на пеленгу 10^o – придушувався на 15 дБ, а сигнал другої завади, що розташовувалась в БЗ на пеленгу -10^o був придушений на 29,4 дБ.

При моделюванні в MathCad просторової селекції сигналів за умови розміщення завад у проміжній зоні на одній лінії з корисним сигналом з метою наближення до реальних умов поширення радіохвиль джерела завад і корисного сигналу розміщені не на одній лінії, а на дуже малому куті розносу (кутове рознесення 1^o). Деякі результати моделювання наведені у табл. 1 при знаходженні ДРВ корисного сигналу на нульовому пеленгу в ДЗ, а ДРВ завад на пеленгах -1^o і 1^o у БЗ відповідно на відстанях 6 і 5 м від АР СМРВ.

Таблиця 1 Результати розрахунків коефіцієнтів придушення

Сигнали	Пеленги сигналів			Придушення, дБ		
	1-й вар.	2-й вар.	3-й вар.	1-й вар.	2-й вар.	3-й вар.
корисний	0^0	$+1^0$	-1^0	8,303	-0,289	-2,325
завада 1	-1^0	0^0	0^0	45	28,491	19,131
завада 2	$+1^0$	-1^0	$+1^0$	37,684	27,123	16,834

Отже з результатів моделювання (табл. 1) можна зробити висновок, що застосувавши просторове розділення сигналів за формами фазового фронту ЕМХ можна досягти доброго придушення завад навіть при відсутності кутового розносу між напрямами приходу корисного сигналу і завад.

Література

1. Техника для спецслужб [Електронний ресурс] – Режим доступу до ресурсу: http://www.bnti.ru.
2. Авдєєнко Г.Л., Корсак В.В., Якорнов Є.А. Модифікація алгоритму Кейпона для визначення пеленгу на джерела радіовипромінювання при сферичних фронтах їх електромагнітних хвиль у місці прийому. Даний збірник.

УДК 621.396.722

ПОБУДОВА СИСТЕМИ НАДШИРОКОСМУГОВОГО ЗВ'ЯЗКУ У ДІАПАЗОНІ 200-400 МГц

Бунін С.Г., Авдєєнко Г.Л., Михайлов С.О.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: moderya7@gmail.com

Building UWB systems broadband in the range 200-400 MHz

Analysis and development of specific technical solutions input stage of receiver UWB signals with a bandwidth of 200-400 MHz. in suite of circuit design programs National Instruments (NI) Multisim. Compare with the theoretical results obtained in Matlab.

Наразі багато уваги приділяється дослідженням надширокосмугових імпульсних Impulse Radio Ultra Wide Band (IR-UWB) сигналів, це зумовлено низкою їх властивостей. Найважливіші з них - це велика пропускна здатність каналів зв’язку, мала середня потужність, споживана терміналами від джерел живлення, завдяки дискретній структурі сигналу та перш за все складність виявлення сигналів (через їхню малу спектральної щільності), що зменшує вірогідність несанкціонованого доступу до інформації, що передається. Ці та інші властивості IR-UWB роблять їх ідеальними для використання у військових системах зв’язку.

У даному тезисі розглядається варіант реалізації вхідного каскаду приймача IR-UWB сигналів.

Діапазон у 200-400 МГц обраний як порівняно ненавантажений іншими службами діапазон, що дозволяє побудувати прототип приймача IR-UWB сигналів з менш жорсткими вимогами по потужності сигналу та виміряти його реальні енергетичні характеристики для перенесення системи у діапазон більш високих частот. Окрім того, елементна база діапазону 200-400 МГц є відносно дешевою, що дозволяє випробувати на практиці більше варіантів побудови схеми на різних елементах.

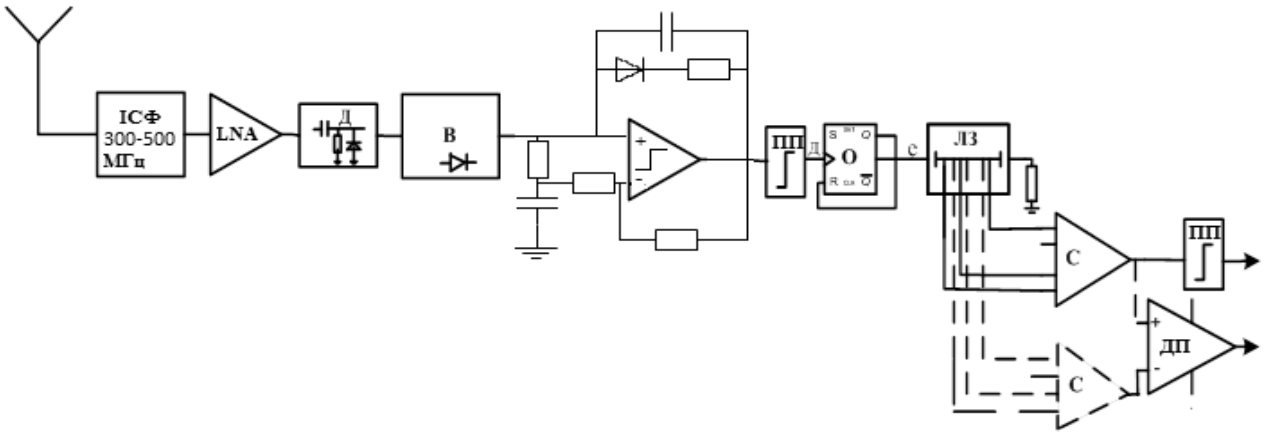


Рис.1 Функціональна блок-схема приймача IR-UWB.

Основу приймача становить запропонована у [1] схема (мал. 1) неенергетичного прийому IR-UWB сигналів, перевагою якої є зниження вимоги до точності розташування відводів у погодженому фільтрі на виході приймача.

У ході даної роботи пропонується виконати на вході схеми приймача розрахований смуговий фільтр Чебишева 7-ого порядку, оскільки саме він при симуляції у NI Multisim дав оптимальний результат. Смугою пропускання фільтра обрано 300-500 МГц, оскільки максимум спектру сигналу, отриманого після приймальної антени знаходиться на частоті 388 МГц. Структура фільтра розрахована у AWR Microwave Office (мал.2).

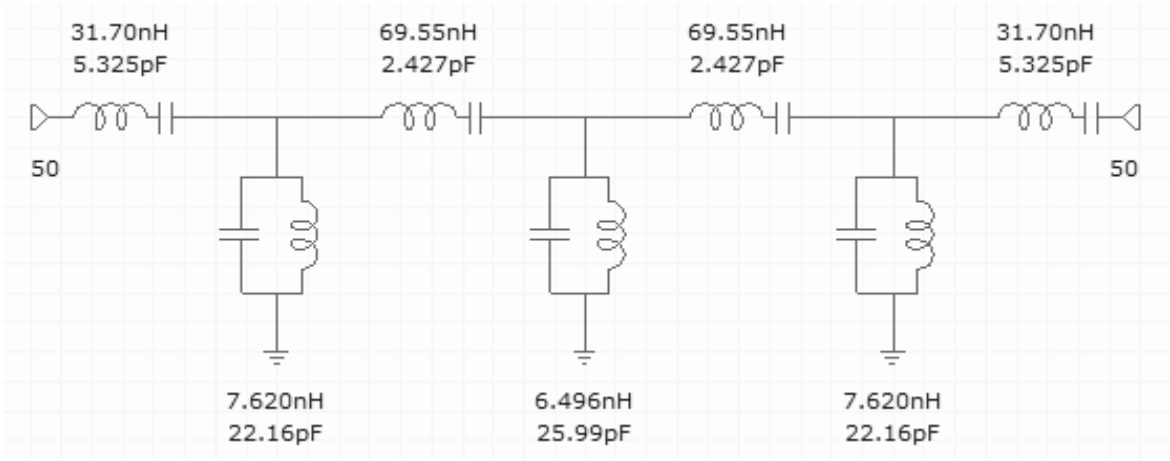


Рис.2 Смуговий фільтр Чебишева 7-ого порядку, зі смугою 300-500 МГц, розрахований за допомогою AWR Microwave Office.

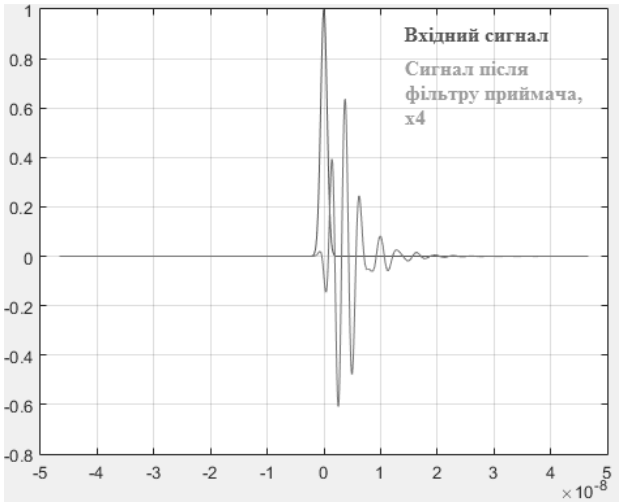


Рис.3 Імпульс з виходу генератора передавача та прийнятий сигнал, знятий після вхідного смугового фільтру приймача, розраховані у Matlab.

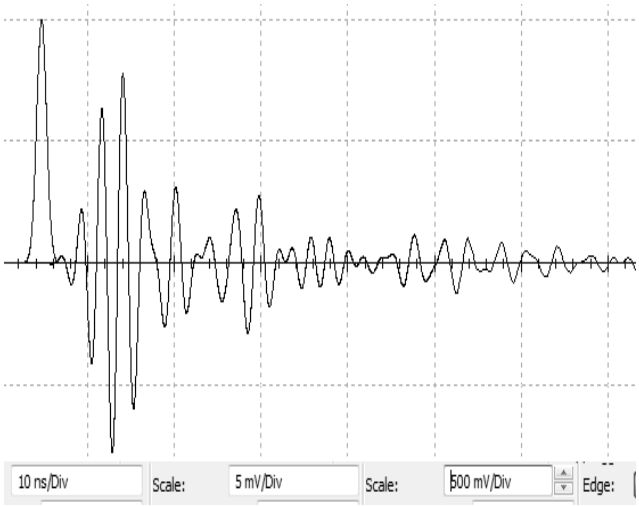


Рис.4 Імпульс з виходу генератора передавача та прийнятий сигнал знятий після вхідного смугового фільтру приймача, розраховані у NI Multisim.

У якості малошумного підсилювача Low Noise Amplifier (LNA) пропонується використати саморобний LNA на основі мікросхеми SPF5043Z (мал. 5). Головною перевагою цього підсилювача є його дешевизна, оскільки SPF5043Z фірми RFMD коштує до 5$. При цьому отриманий LNA має достатнє підсилення (22,8 дБ на 144 МГц, 20,5 дБ на 432 МГц) і малий коефіцієнт шуму (0,6 дБ на 144 МГц , 0,65 дБ на 432 МГц) [2].

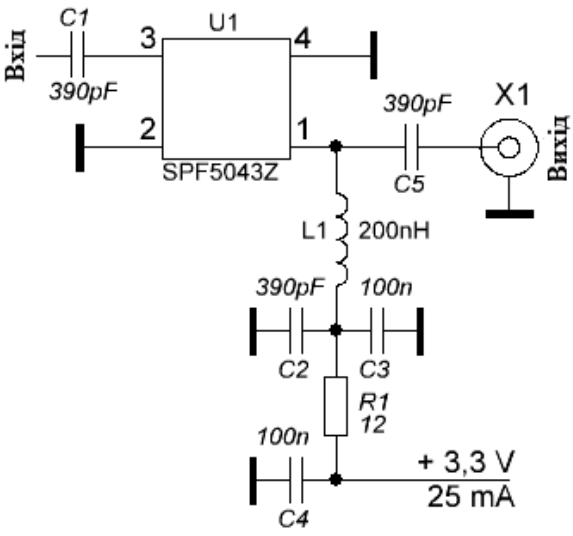


Рис.5 Принципова схема LNA на основі мікросхеми SPF5043Z

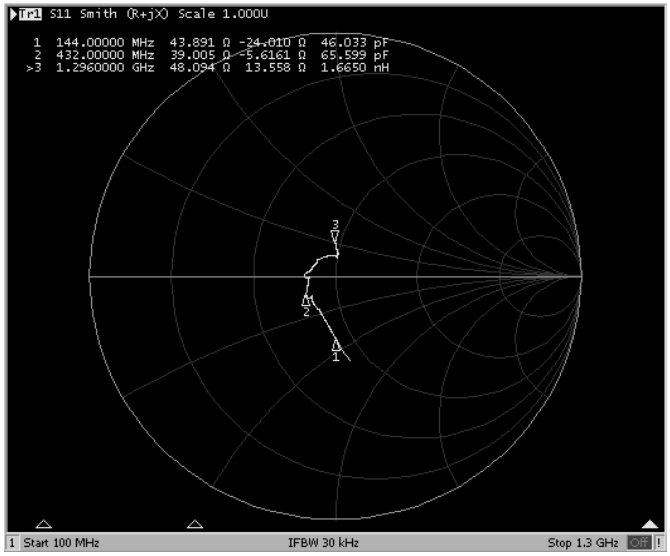


Рис.6 Графік комплексного вхідного навантаження LNA

Проте даний підсилювач має значний мінус – він не є надто широкосмуговим, що видно на мал. 6. Однак, зважаючи на те, що даний приймач служить лише для оцінки енергетичних параметрів системи, використання даного LNA може бути допущене, оскільки переоцінка втрат, зумовлених коефіцієнтом стоячої хвилі не є негативним фактором оцінки параметрів приймача, ці втрати можна вважати певним енергетичним запасом.

Література

1. ‘Non Energy’ Reception of Ultra Short Impulse Signals/ Sergey Bunin Institute of Tetelecommunications of the National Technical University of Ukraine “KPI”, Ukraine, 2010, 4 ст.
2. Антенный VHF усилитель [Электронный ресурс]: многопредмет. науч. форум / – Электрон. журн. – Dimona: 11.09.2012. - . – режим доступу до форуму.: http://dl2kq.de/ant/3-64.htm

УДК 621.382

РАЗРАБОТКА УДВОИТЕЛЯ МИЛЛИМЕТРОВОГО ДИАПАЗОНА

Половий О.М, Приступчук Ю.А., Шелковніков Б.М.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: OleksandrPolovyiPublic@gmail.com

Design of doubler MM-WAVE

This article presents the results of frequency doubler 60 GHz - 120 GHz based on HEMT technology simulations by using AWR packet. The results allow to move to the next stages - topology development and technological implementation.

Интерес к системам, работающих на частотах выше 100 ГГц непрерывно растет. Применение варьируются от атмосферной радиометрии до автомобильных, радиолокационных, сенсорных и телекоммуникационных систем [1-4].

Основной задачей для систем, работающих в данном диапазоне частот, является оптимальный выбор источников сигнала с низким энергопотреблением, широкой полосой и возможностью интеграции с остальной системой. Наиболее распространенным способом является использование высокопроизводительного источника сигнала, работающего на низких частотах вместе с умножителями с надлежащим усилением, что позволяет получить сигнал желаемой частоты и мощности. Поэтому разработка умножителей для систем, работающих на частотах выше 100 ГГц является актуальной.

Системы строятся на основе устройств в состав которых входят умножители и к ним предъявляются требования от этих системЭта статья представляет результаты моделирования удвоителя частоты 60 ГГц - 120 ГГц в ПС AWR. Схема выполнена по технологии GaAsmHEMT 0.06-0,1 мкм с типичными параметрами $(G_m)_{max}$= 1400 mS/mm, $(ID)_{max}$= 900 mA/mm и f_t и F_{max} 200 ГГц и 300 ГГц соответственно [1].

Умножение частоты достигается за счет нелинейностей транзисторов. В умножителях, на основе полевых транзисторов, транзистор смещен таким образом, что РЧ-сигнал от тока стока содержит гармоники частоты входного сигнала. Желаемая частотная составляющая фильтруется на выходе, а нежелательные составляющие подавляются. В большинстве случаев, необходимая частотная составляющая имеет недостаточный уровень мощности, поэтому впоследствии она должна быть усилена.

Удвоитель частоты использует полевой транзистор, работающий в режиме класса АВ в состоянии покоя, т.е. напряжение на затворе находится близко к пороговому значению, так что гармоническая составляющая второго порядка присутствует в выходном сигнале тока транзистора.

Рассмотрим на рис.1 структурную схему удвоителя частоты 60 ГГц - 120 ГГц, которая была разработана в среде AWR.

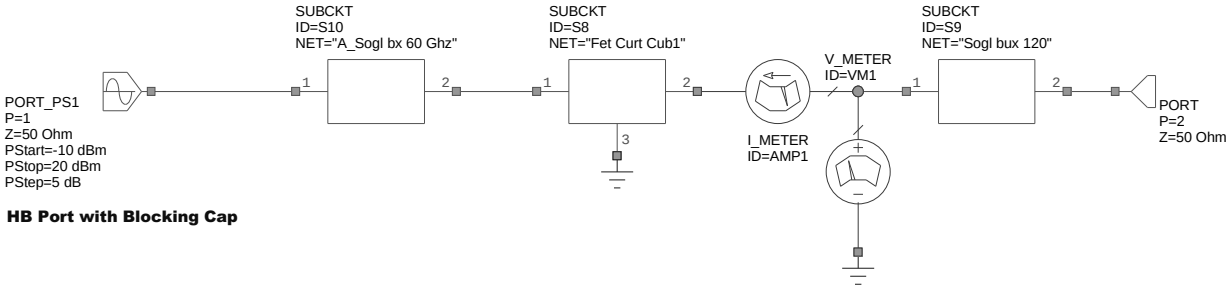


Рис. 1 Структурная схема каскада удвоителя.

Схема каскада состоит из согласующей цепи на 60 ГГц (рис.2), полевого транзистора и согласующей цепи на 120 ГГц (рис.1).

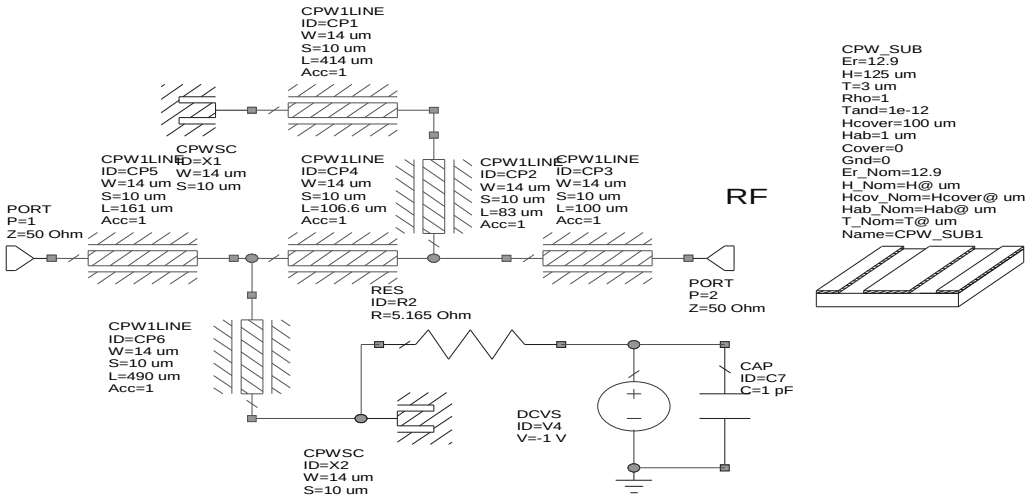


Рис. 2 Схема согласующей цепи на 60 ГГц.

Фильтр на выходе устраняет нежелательные гармоники. Результаты моделирования и основные показатели приведены на рисунках ниже:

На рис.3 приведены графики вольт-амперной и динамической характеристики каскада, а также на рис. 4. приведены графики мощности сигнала на выходе схемы как функции входной мощности.

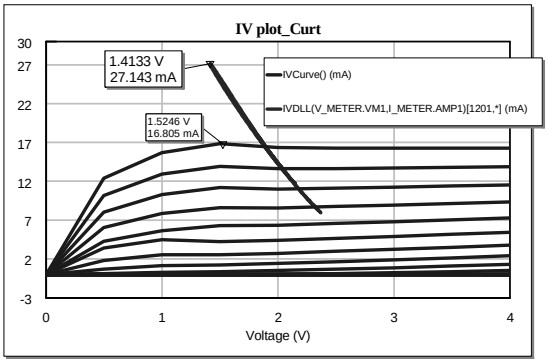


Рис. 3 Вольт-амперная и динамическая характеристики каскада/

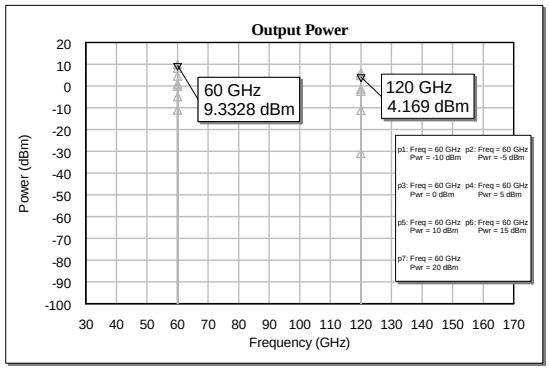


Рис. 4 Выходная мощность сигнала на выходе схемы/

На рис. 5 приведен график потерь преобразования как функция мощности на входе от частоты, а также на рис. 6. приведены временные характеристики тока и напряжения схемы.

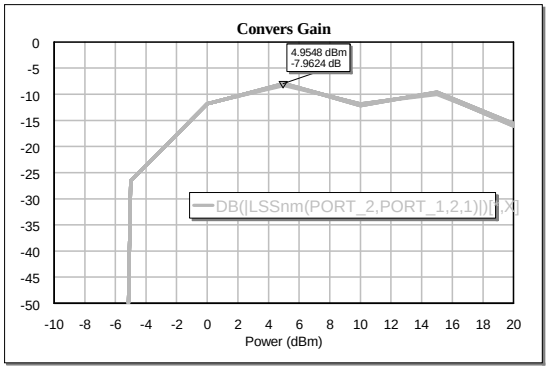


Рис.5. Потери преобразования

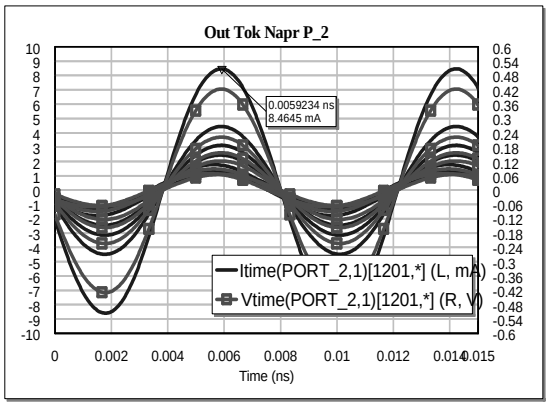


Рис.6. Временные характеристики тока/напряжения схемы

Результаты моделирования показывают, что схема удвоителя частоты 60 ГГц - 120 ГГц удовлетворяет предъявляемым требованиям, и на основе такого удвоителя возможно приступать к проектированию топологии и технологической реализации**.**

Промоделирована работа HEMT удвоителя частоты 60 ГГц - 120 ГГц, определены основные его качественные показатели и характеристики. Они удовлетворяют предъявляемым требованиям от беспроводных систем.

Литература

1. Teiwes M. Electronic integrated circuits and modules for high frequencies [Електронний ресурс] / Michael Teiwes. – 2015. – Режим доступу до ресурсу: http://www.iaf.fraunhofer.de/en/research-projects/high-frequency-electronics.html.
2. Pozar D. M. Microwave Engineering / D. M. Pozar. – . New York: Wiley, 2005. – 143 с.
3. Akihiko H. 120-GHz-Band Millimeter-Wave Photoni Wireless Link for 10Gb/s Data Transmission / H. Akihiko, K. Toshihiko, T. Hiroyuki. // IEEE Transactions on micro-mave theory and techniquos. – 2006. – №54. – С. 11–15.
4. Radisic V. 164-GHz MMIC HEMT Doubler / V. Radisic, M. Micovic, M. Janke. // IEEE Microwave and Wireles Components Lett. – 2001. – №11. – С. 241–243.

УДК 621.39

АПРОКСИМАЦІЯ ХАРАКТЕРИСТИК РАДІОЛІНІЇ ДОСТУПУ В САНТИМЕТРОВОМУ І ДЕЦИМЕТРОВОМУ ДІАПАЗОНАХ

Воловик А.О., Бунін С.Г.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: volovykandrey@gmail.com

Approximation of access radioline characteristics in the centimeter and decimeter ranges

Designed an efficient method for approximating the empirical characteristics radio wave attenuation in the propagation models in urban environments, as well as AFC experimental radio links based on electrical theory filter theory and numerical methods.

Для розробки моделюючого фільтру при оцінці передачі потужності Ultra - Wide Band (UWB) сигналу в зону прийому можна використовувати метод апроксимації будь-якої, в тому числі емпіричної, частотної характеристики радіолінії [1] .

При вирішенні задачі апроксимації можна використовувати різні критерії, які застосовуються при синтезі фільтрів в теорії електричних ланцюгів, якщо апроксимувати АЧХ радіолінії перехідною смугою фільтра [2] . Однак необхідно враховувати, що рішення такого завдання є компромісом між ідеальною формою апроксимуючої функції і складністю її використання при аналізі та синтезі систем і сигналів. Отже, беручи до уваги гладкість кривих ослаблення відповідно до моделі Окамури-Хата [3] застосуємо апроксимацію поліномом якомога нижчого порядку.

Для прикладу візьмемо нижню частоту радіолінії, що моделюється $f_н = 500 МГц$, верхня частота $f_В = 1500 МГц$, тоді гранична частота смуги пропускання $f_П = f_Н$, а полоси затримки $f_З = f_В$; дальність зв'язку $d = 5км$, висота приймальної і передавальної антен відповідно $h_{прм} = 2м$ та $h_{прд} = 30м$. Значення ослаблення вичислимо по методиці Окамури-Хата. Для отримання універсальних результатів проводимо нормування частоти і ослаблення радіолінії. Далі визначаємо для синтезу ФНЧ-прототипу допустиме загасання в полосі пропускання $A_{\max}$ і в полосі затримки $A_{\min}$.

Проведемо проміжне перетворення по частоті, нормуюче область частот: $\Omega = f / f_Н$, де f = (500 1000 1500) МГц, тобто отримаємо Ω = (1 2 3), тоді медіанне ослаблення у відповідності до моделі Хата для міста буде $A_М$ = (143.2 155.9 165.4) дБ.

Додаємо корегуючий коефіцієнт типу місцевості [3] . Знаходимо:
A = (159.2 176.9 182.4) дБ або після нормування A = (1 17,7 23,2) дБ, що відповідає квадрату АЧХ $H^2(\Omega) = 10^{-0,1A(\Omega)}$ = (1 0,017 0,004786). Далі, задаючись допустимим ослабленням в смузі пропускання ФНЧ-прототипу, наприклад 3дБ, тобто $A_{\max}$ = 3дБ, визначаємо допустиме затухання в полосі

затримки $A_{\min}$ = 23,2дБ.

У відповідності з методом поліноміальної апроксимації теорії електричних фільтрів передавальна функція моделюючого ФНЧ – прототипу має вигляд [4] :

$$H(p) = \frac{1}{V(p)}, \tag{1}$$

де $V(p) = p^n + a_1 p^{n-1} + ... + a_{n-1} p + a_n$ - поліном Гурвіца.

Ослаблення поліноміального фільтра є чіткою функцією нормованої частоти:

$$A(\Omega) = 10\lg\frac{1}{\left|H(j\omega)^2\right|} = 10\lg(A_0\Omega^{2n} + A_1\Omega^{2n-2} + ... + A_n), \tag{2}$$

де Ω - нормована частота відносно частоти $f_П$.

Коефіцієнт ослаблення ФНЧ-прототипу при гладкій апроксимації дорівнює:

$$A(\Omega) = 10\lg(1 + A_0\Omega^{2n}). \tag{3}$$

Відомо, що фільтри з такими характеристиками ослаблення називаються фільтрами з характеристиками Баттерворта [5] . Якщо $A_{\max}$ = 3 дБ, то A_0= 1. Далі знаходимо передаточну функцію фільтра:

$$H(p)\cdot H(-p) = \left|H(j\omega)\right|^2_{j\omega=p} = \frac{1}{1+(-jp)^{2n}}. \tag{4}$$

Обчислюємо корні рівняння $1+(-jp)^2 = 0$; відібравши полюси, що відносяться до $H(p)$, отримаємо:

$$H(p) = \frac{1}{\sum_{k=1}^{n}(p - p_k)} = \frac{1}{p^n + a_1 p^{n-1} + ... + 1}. \tag{5}$$

Синтез ФНЧ-прототипу проводимо у відповідності з представленою вище методикою. Його передавальна функція визначається формулою:

$$H(p) = \frac{1}{p^3 + 2p^2 + 2p + 1}. \tag{6}$$

Далі, здійснюючи стандартну заміну змінних, отримуємо відповідну динамічну модель радіолінії у вигляді передавальної функції апроксимуючого смугового фільтра:

$$H_{an}(p) = \frac{p^3}{p^6 + 2p^5 + 5p^4 + 4p^3 + 5p^2 + 2p + 2}. \tag{7}$$

Робоче ослаблення моделі радіолінії шостого порядку в характерних точках буде *A* = (0 12 25) дБ. Максимальне відхилення в середній точці від реального ослаблення складає суттєву величину (більше 5 дБ). Головним недоліком цієї моделі є недостатня точність симетричної моделі досить високого порядку.

Для апроксимації несиметричного загасання в області низьких і високих частот, а також для підвищення точності, можна модернізувати розглянутий метод. Зокрема, синтезувати один ФНЧ-прототип для області низьких частот, а

інший – для високих частот. Тоді модель АЧХ несиметричної радіолінії може бути представлена у вигляді різниці АЧХ отриманих ФНЧ. Таким чином, ослаблення радіолінії моделюється різницею двох трапецій низькочастотного ослаблення. На рис. 1 приведені АЧХ (суцільна лінія – модель радіолінії, штрихова і пунктирна відповідають допоміжним моделям ФНЧ1 і ФНЧ2). Визначаємо АЧХ двох допоміжних ФНЧ-прототипів по характерним точкам в області низьких частот і в діапазоні радіолінії $(H_1(\Omega))$ і $(H_2(\Omega)$ на рис. 1).

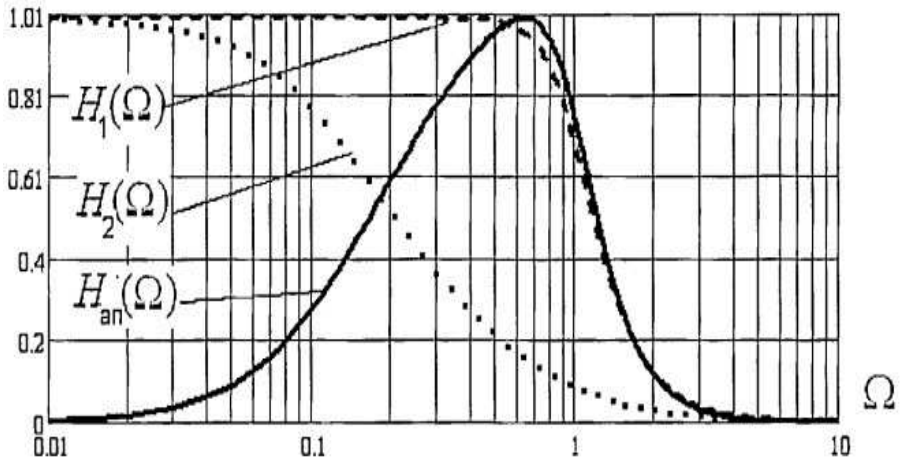


Рис. 1 АЧХ динамічної моделі по методу трапецій.

Далі по методу двох трапецій приходимо до необхідної моделі радіолінії, АХЧ якої знаходиться як різниця відповідних характеристик ФНЧ-прототипу $(H_1(\Omega) - H_2(\Omega))$.

Отримана методом трапецій модель радіолінії в діапазоні частот апроксимацій має ослаблення *A* = (2,2 18 30) дБ. Якщо здійснити перетворення нормованих частот $\Omega_1 = \Omega - 0{,}35$, то шкала частот буде відповідати першій моделі. В цьому випадку ослаблення буде
A = (0 13,9 27,1) дБ. Максимальне відхилення в середній точці від реального ослаблення дорівнює близько 4 дБ.

Висновок: Другий метод апроксимації має більшу точність і дозволяє описувати радіолінії з несиметричними АЧХ. Однак, як і метод смугового фільтру (перший метод), метод трапецій гарантує точність лише в одній точці апроксимуючої АХЧ радіолінії.

Література

1. Комашинский В.И., Максимова А.В. Системы подвижной радиосвязи с пакетной передачей информации. Основы моделирования. - М.: Горячая линия - Телеком, 007-176с.
2. Бабков Ю.В., Вознюк М.А., Михайлов П.А. Сети мобильной связи. Частотно - территориальное планирование. - М.: Горячая линия - Телеком, 2007. - 224с.
3. H. L. Bertoni, Radio Propagation for Modern Wireless Systems, Upper Saddle River, NJ: Prentice Hall, 2000.
4. Урядников Ю.Ф., Штыркин В.В. Технология сверхширокополосного абонентского доступа по проводным линиям. - Электросвязь, 2004, №6, С. 27-31.
5. Хазел Г.Е. Справочник по расчету фильтров. Пер. с англ. под ред. А.Е. Знаменского. - М. "Сов. радио", 1974, 288с.

Секція 8. Підготовка кадрів телекомунікаційного профілю, історія розвитку телекомунікацій.

Секцію 8 об'єднано з Секцією 2.

Секція 9. Modern information and telecommunication trends

UDC 621/39

LATVIAN EXPERIENCE: THE COMPARATIVE REVIEW OF STUDY ABROAD VIA THE ERASMUS+ PROGRAMME

Hanna Hakhova
Institute of Telecommunication Systems, NTUU "KPI", Ukraine
E-mail: anna.gakhova@gmail.com

Досвід з Латвії: Порівняльний огляд навчання за кордоном крізь призму програми Еразмус +

Дана стаття присвячена огляду проходження навчання за кордоном у рамках програми обміну Еразмус+, а саме у Ризькому технічному університеті (РТУ) у Латвійській Республіці. У статті розглянуто різні аспекти навчальної та освітньої діяльності у РТУ та висловлено спостереження щодо особливостей навчання у європейському вищому навчальному закладі.

This article is dedicated to study process abroad at Riga Technical University (RTU) in the Republic of Latvia as a part of Erasmus + programme during the fall term of 2015. There is a wide range of engineering specialties offered to the students of RTU, and as a Telecommunications student, the preference was given to the Faculty of Electronics and Telecommunications (FET).

There were several goals to achieve during the study abroad, such as:

- to get familiar with the study programme of another university;
- to try out some new learning strategies;
- get additional knowledge in related branches;
- to improve communication skills in the English language.

First of all, I would like to share my observations of the study process in general. Learning takes place in the familiar form of lectures, seminars and practical work I was accustomed to at KPI. However, first striking difference is the number of disciplines, which is noticeably fewer than at KPI. It means that overall spectrum of knowledge and skills gained by studying at RTU is considerably narrower, but on the other hand, some fields may be understood on a deeper level. I found out that it was easier to focus on separate disciplines.

The time allotted for studying at RTU was limited but I had an opportunity to take a glimpse at the scientific side of life there. From time to time representatives from various European universities and organizations visit RTU. For example, I was able to attend CERN seminars about the Large Hadron Collider and the Higgs boson.

Various conferences are also held at RTU and I participated in one of them: the 56th International Scientific Conference, Telecommunications section. It was quite positive experience as it turned out that I was the only attendee who did not understand Latvian so the language of conference was changed to English despite the fact that everyone initially prepared the report in Latvian.

Another interesting but somewhat difficult aspect of studying at RTU was multinationality of Erasmus + participants. The students in my group were from India, Nigeria, Spain, Nepal, Egypt and it was not always easy to communicate with them. A lot of attention was paid to teamwork, but unfortunately, it was quite hard to establish a common language in a multicultural team to perform a task efficiently. (I precisely felt the meaning of the legend about the Tower of Babel).

It is worth mentioning the priority directions of research and educational activity at the Faculty of Electronics and Telecommunications in particular. I can highlight the major fields of study:

1) Fiber-optic Communication Systems;

2) Mobile Communication Systems.

The greatest emphasis is placed on Fiber-Optic Communication Systems. Broad arsenal of telecommunication equipment can be found inside the building of FET and every student is authorized to use it not only within the study programme, but also beyond it, for his or her own educational and research needs.

Unsurprisingly, the examination process is similar to KPI's with familiar acquisition of points during the term and final examination session. At the end of the term students take part in a survey and they evaluate different aspects of lecturers' work. It is very substantial process and a lot of attention is paid to it. It is interesting to see if such a practice becomes important in KPI.

In conclusion, I can say that my goals were achieved. I definitely gained a positive experience, significantly developed communication skills in the English language and listened to an interesting course of lectures.

In general, the Academic mobility is an integration process in education which enables students, graduates and teachers to participate in different educational or researching programs. The main purposes of such programs are increase of education quality, development of intercultural exchange, training of future qualified specialists. Participation in the academic mobility programs gives students an opportunity to get good European education in the chosen field, to broaden their knowledge in all fields of European culture, to feel themselves as native Europeans. Today the KPI students can get an experience of being a part of a completely different educational system. Cooperation is based on KPI partnership with foreign universities and companies, due to which our students can participate in international education programs.

Academic mobility became an essential part of modern education and its role is constantly growing.

УДК 621.396.94

DATA PROCESSING AND STORAGE IN THE INTERNET OF THINGS SYSTEMS

Kurdecha V. V., Ishchenko I. I., Zakharchuk A. G.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: ishchenko.io@yandex.ru

ОБРОБКА І ЗБЕРІГАННЯ ДАНИХ В СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ

У статті був проведений аналіз існуючих технологій до появи IoT Hub. Було підтверджено підвищення ефективності та безпеки обробки даних в системах Internet of Things за рахунок нової IoT архітектури з використанням IoT Hub.

In the paper, an analysis of existing technologies before the emergence of IoT Hub is presented. The increase of efficiency and security of data processing in the Internet of Things systems through a new IoT architecture using IoT Hub was confirmed.

The Internet of Things (IoT) in future will bring together billion devices called “smart things”. These devices can be extremely heterogeneous in terms of hardware (e.g. processing power and available memory), software (e.g. operating systems, application software (middleware)) and communication interfaces. The purpose of our work is to improve the efficiency and security of data processing in the Internet of Things systems through a new IoT architecture using IoT Hub.

IoT Hub has advantages compared with earlier IoT services such as Eventhub and service bus. It is able to receive messages from device to cloud service (Telemetry messages, feedback), as well as sending messages and commands from devices to cloud services. It allows us to manage, monitor and connect the huge number of devices supporting HTTP, AMQP and MQTT protocols. SDK available for multiple platforms such as Windows, Linux and some RTOS and support multiple languages such as C, .NET, Java and Node.js. In view of the above considerations, it is proposed to use the node named as “IoT Hub”, which enhances the network by implementing as follows: a router, Cross-proxy, cache and a directory of resources. In design work the method of processing and data storage IoT systems. IoT Hub is designed to connect devices easily to the cloud service and provide two-way communication (device - cloud services, cloud services - the device). This bidirectional message will be securely stored and authenticated, thereby ensuring security and privacy. In addition, IoT Hub provides access to libraries for the most popular languages and platforms that provide tools in order to safely and securely connection. Figure 1 shows the architecture of our proposed solutions for data processing and storage in the IoT

systems. The proposed architecture with additional node IoT Hub provides the ability to handle millions of requests per second per processor events, and IoT Hub stores data about events for up to seven days to ensure reliable processing. IoT Hub provides authentication for each device and a secure connection. We can provide our own security for each device key used to connect to the center of the IoT.

Register of certificates IoT center stores device IDs and keys in the decision. The server part of the application solutions can add individual devices to the whitelist or blacklist, thereby completely controlling access devices.

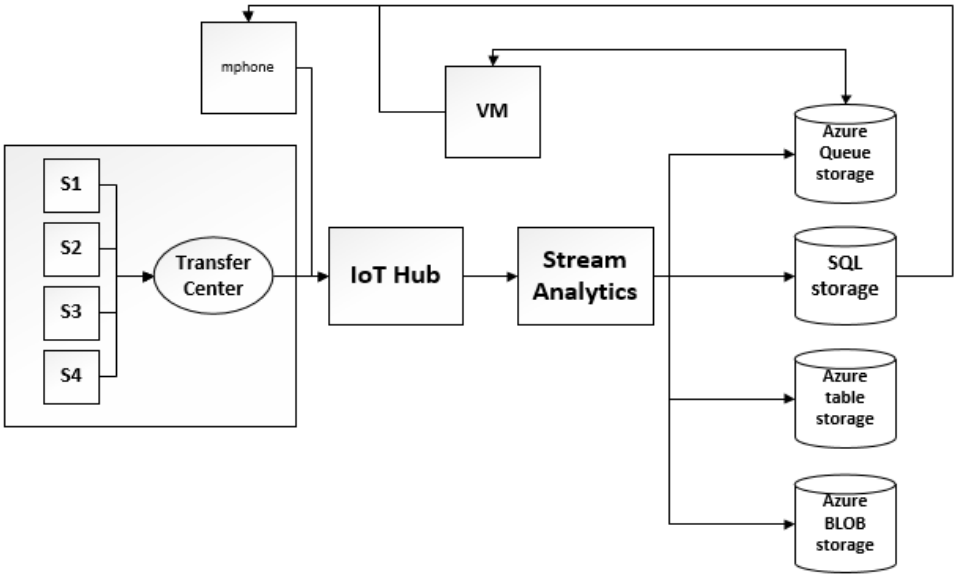


Fig. 1 System IoT architecture using IoT Hub.

Fig. 1 shows the architecture of the following elements:

1. S1, S2, S3, S4 - a set of sensors.
2. Transfer Center - serves as a device that sends data from all sensors simultaneously to IoT Hub.
3. IoT Hub - provides opportunities messaging between devices and cloud services, and acts as a gateway to the cloud and other key services IoT Suite.
4. Module event processing Azure Stream Analytics provides rapid data analysis. This is a service for handling incoming data telemetry, aggregation and detection of events.
5. To store data and their preparation for analysis of preconfigured storage solution using BLOB-objects, Queue-, SQL-, table-storage.
6. Data visualization capabilities available web applications Azure and Microsoft Power BI, which are designed and configured by virtual machine.

To store text and audio of any type of storage used by BLOB-objects such as documents or media files. Repository tables – a key store and attributes. There are fast and economical access to data provided by the applications of all kinds. Telemetry data scanned from the sensors are transmitted using Raspberry Pi microcomputer input service IoT Hub. Then the incoming data is analyzed, broken down into flows analyzed for the presence of abnormal data and recorded in various repositories. Analysis of business requirements led to the conclusion that the data telemetry health indicators recorded as a current day. Information is better seen in graphs that are generated using Power BI. Formation of graphs is a cloud service Azure, so to save the data, we can use table-storage. Due to the large processing power Azure offset disadvantages of slow reading and processing.

In this paper we have presented the analysis of existing technologies before the emergence of IoT Hub and the advantages of using cloud services for data processing and storage in IoT systems using such a technology as IoT Hub. The IoT Hub can be used by external clients to discover and access smart objects without requiring any a-priori knowledge of their details (e.g. communication protocol and IP address). It is also able to manage a number of heterogeneous physical networks, each with several devices, with limited use of resources, in terms of processing and memory, thus making it possible to deploy the IoT Hub even on low-end devices.

References

1. K Dostert, 1997, Telecommunications over the Power Distribution Grid-Possibilities and Limitations Proc 1997 Internat. Symp. on Power Line Comms and its Applications pp1-9 [2] R Broadridge 'Power line modems and networks' 4'th International Conference on Metering Applications and Tariffs for Electricity Supply IEE conf., London.
2. I. Ishaq, J. Hoebeke, I. Moerman, and P. Demeester, “Internet of Things Virtual Networks: Bringing Network Virtualization to Resource-Constrained Devices,” in Green Computing and Communications (GreenCom), 2012 IEEE International Conference on, Nov 2012, pp. 293–300.
3. M. Aazam, P. P. Hung, and E.-N. Huh, “Smart gateway based communication for cloud of things,” in Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2014 IEEE Ninth International Conference on, April 2014, pp. 1–6.
4. M. Aazam and E.-N. Huh, “Fog Computing and Smart Gateway Based Communication for Cloud of Things,” in Future Internet of Things and Cloud (FiCloud), 2014 International Conference on, Aug 2014, pp. 464–470.

UDC 621.39

THE INTERNET OF THINGS (IOT) SYSTEMS CONTAINING NOMADIC UNITS ARCHITECTURE MODIFICATION AND THE MOST RATIONAL TECHNOLOGIES SELECTION

Kurdecha V.V., Gvozdetska N.A., Zvonarov O.V.
Institute of Telecommunication Systems NTUU "KPI"
E-mail: n.gvozdetska@gmail.com

Архитектура системы Internet of Things (IOT) содержащей мобильные (подвижные) узлы

В работе описана архитектура системы Internet of Things (IoT) содержащей мобильные (подвижные) узлы. Для систем такого типа предложен вариант использования существующей инфраструктуры сети сотовой связи, а именно использование технологии GPRS для передачи данных между мобильным узлом и облачным сервисом. В работе также осуществлен подбор рациональных протоколов для передачи данных от мобильного узла к облаку на прикладном уровне модели OSI.

Introduction. The IoT is expected to have great impact on several aspects of our everyday-life, enabling the development of a wide range of applications, including: sensor data aggregation, intelligent transportation schemes, business management, environmental monitoring, e-health and many others [1].

This paper is dedicated to analysis and comparison of protocols and technologies which are the most appropriate for devices interconnection. The entire system structure building is proposed.

There are a lot of solutions for IoT systems containing only static units. The structure of these systems is defined and is shown on the figure 1.

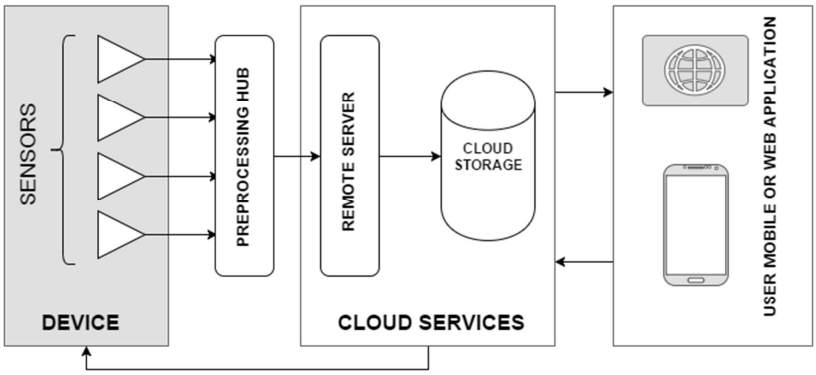


Fig. 1. "General structure of the typical IoT system".

For systems with nomadic units have been also proposed some decisions. One of them is new 3GPP Standard for IoT – a special technology to address the requirements of the IoT. The new technology will provide improved indoor coverage, support of a massive number of low-throughput devices, low delay sensitivity, ultralow device cost, low device power consumption, and optimized network architecture [2]. This technology has a great potential of development, but

this paper is aimed to find a solution based on usage of more common technologies for narrow range of systems. For such kind of system implementation there is no common developed infrastructure yet. To make a decision universal it is a need to use existing infrastructure.

Proposed architecture for systems with nomadic units. The mobility of these nomadic units can be considered in different areas of application. Talking about the Smart House conception, mobility is presented only within the home. It doesn't cause any essential problems because a majority of the modern houses are provided with some kind of network (usually it can be IEEE 802.11 (Wi-Fi) network or IEEE 802.15 (Bluetooth) network). But these technologies are not suitable for a number of IoT systems that require their units' interconnection at large distances.

According to this statement it is suggested to modify architecture to provide a connectivity of standalone nomadic unit using existing mobile networks. The structure of such system is shown on the figure 2.

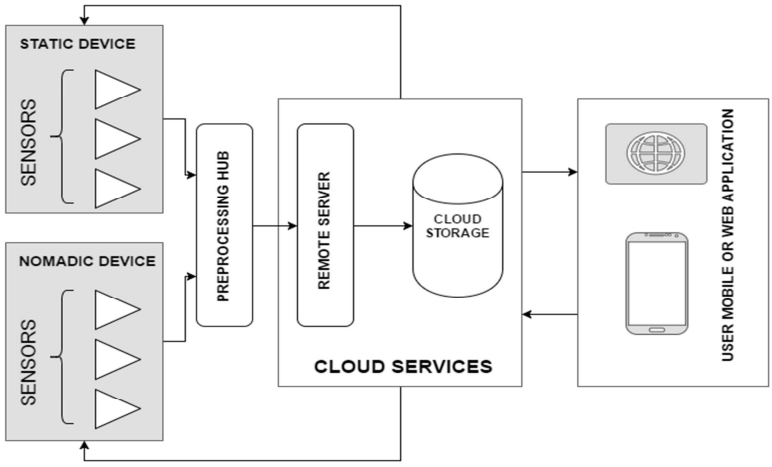


Fig. 2. "General structure of the IoT system including nomadic units".

The protocols of the network and transport layer of the OSI model for both variants of system configuration are quite definitely specified. Being an Internet using system, IoT uses TCP/IP stack of protocols on these layers. But there are some problems with an application and physical layers as the endpoints of the IoT system are smart devices.

1.1. Physical layer technologies.

It is necessary to provide a stable connection wherever the nomadic unit is. IEEE 802.11 Wi-Fi and IEEE 802.15 Bluetooth technologies are not suitable to use as their coverage area is extremely small. The best choice in today's situation is to use mobile GPRS, CDMA, HSPA (for 3G-networks), LTE or other like standards.

The data which is typically transferred is a couple of parameters definitions taken from the sensors. It means that the GPRS capabilities are completely enough for such systems. The infrastructure all over the world is quite developed to make a usage of this technology possible.

The advantages of the GPRS using in the IoT systems with the nomadic units:

1. Sufficient rates;

2. Developed infrastructure;
3. Density and common use;
4. Economic efficiency.

The disadvantages of the GPRS using in such systems:

1. Not enough capabilities in case of a big amount of data transferring;
2. Obsolescent technology in comparison with LTE and the others.

In the proposed solution GPRS technology was used that allows to use existing mobile telecommunication infrastructure.

1.2. Device-to-Cloud and Cloud-to-Device interaction ways.

The most widely used in the IoT systems protocols are AMQP (Advanced Message Queuing Protocol), MQTT (Message Queue Telemetry Transport) and HTTP or HTTPS (HyperText Transfer Protocol Secure).

Being the most universal, HTTP is widely used in the IoT systems, but it uses its potential rather in the device-to-cloud interaction than the nomadic-to-static units' connection. Its advantages are simplicity, universality and security (talking about the HTTPS). But it is not really adapted for the IoT systems.

In comparison to the HTTP/HTTPS, AMQP is used in the IoT systems rather due to its reliability and interoperability than the universality. The disadvantage of AMQP is that it is suitable mostly for the control plane or server-based analysis functions. It is good to be used between the device and cloud to provide efficient way of queues organizing and reliable messaging, as AMQP is aimed to avoid any losses of messages.

The most adapted to the IoT features is MQTT protocol. As its name states, its main purpose is telemetry, or remote monitoring.

In the proposed solution the MQTT protocol is used because being developed especially for IoT it matches all of the requirements to the IoT system units' proper interaction.

Conclusions

1. In this paper is suggested the approach to the IoT systems containing nomadic units design. This approach allows to use existing technologies efficiently;

2. The aspects of physical layer interaction (concerning mobile unit existing in a system) were researched. The way of interaction using existing mobile networks was proposed;

3. Device-to-Cloud and Cloud-to-Device communication ways are investigated and the most appropriate protocols were chosen.

References

1. Michalis Giannikos, Korina Kokoli, Nikos Fotiou, Giannis F. Marias and George C. Polyzos "Towards Secure and Context-Aware Information Lookup for the Internet of Things" International Conference on Computing, Networking and Communications, Communications and Information Security Symposium, 2013.
2. Javier Gozalvez "New 3GPP Standard for IoT IEEE" vehicular technology magazine, Mobile radio, |March 2016.
3. Roberto Verdone, "Internet of Things: How to Break the Barriers for Business Development", 3th International Black Sea Conference on Communications and Networking, 2015.

UDC 621.39

BORDERS CALCULATION OF OPTIMIZATION PARAMETERS CHANGES AT SYNTHESIS OF A SATELLITE DISTRIBUTION NETWORK

E.S.Svetsinskaya, K.S.Sunduchkov
Institute of Telecommunication Systems, NTUU "KPI", Ukraine
E-mail: e.svetsinskaya@hotmail.com; k.sunduchkov@gmail.com

Расчет границ изменения параметров оптимизации при синтезе спутниковой распределительной сети

В работе представлены границы изменения параметров оптимизации при синтезе спутниковой сети распределения ТВ-программ в Украине. В качестве параметров оптимизации приняты три основных потребительских параметра: количество программ (каналов) вещания; качество вещания; цена создания радиотехнической части сети.

The paper presents borders of optimization parameters changes at synthesis of satellite distribution network of TV programs in Ukraine. As optimization parameters there are three main consumer parameters: number of programs (channels) of broadcasting; quality of broadcasting; cost of creating a radio part of the network.

I. Introduction. While designing the satellite distribution network of TV programs we are dealing with a large number of conflicting parameters that have both different dimensions and contradictory effects on the target function of system.

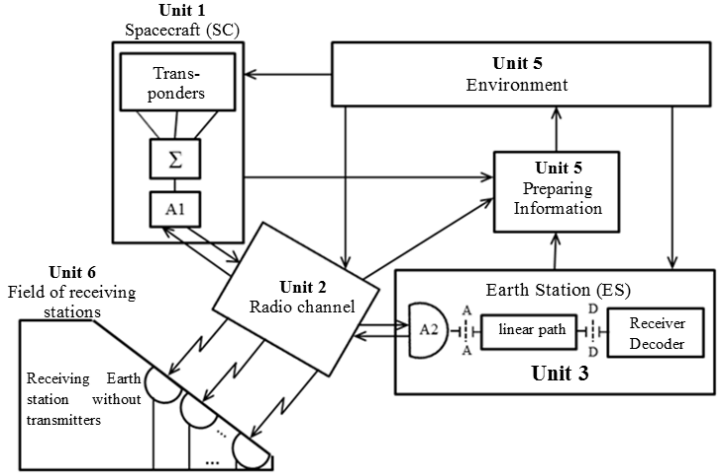


Fig.1. Block diagram of aggregate model of the system of satellite distributed network TV-programs.

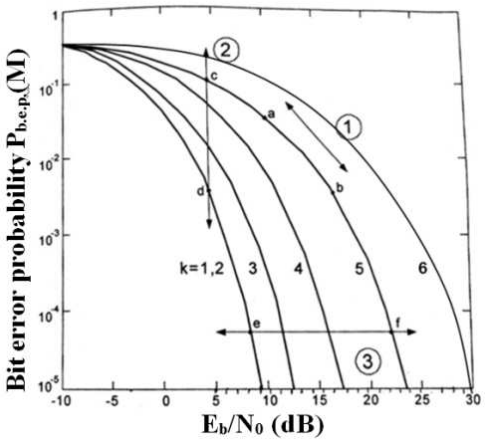


Fig. 2. The dependence of the bit error probability on ratio Ps/Pn at the input of the receiver-decoder of the Earth station satellite signal reception.

Technical requirements for the state network of satellite broadcasting TV-programs on the territory of Ukraine:

1. 400 programs (number of channels).
2. The quality of broadcast must conform to the following requirements: the

transmission quality 4:2:2; the reception quality $P_{b.e.p.} \leq 10^{-5}$.

3. The cost of creating the network should be minimal, along with the cost of a transponder must be no more than 50000 $ USA.

The scheme of the research object

Fig. 1 introduces a newly developed structural diagram of aggregate model of the distribution channels.

II. The general formulation of optimization problem. Based on the terms of reference, target optimization parameters are denoted as follows:

y_1^* - the number of channels in the network;

y_2 – the quality of signal reception (estimated probability of bit error receiver - decoder) for the given transmission quality (quality of transmission = 4:2:2);

y_3 – cost of equipment.

For details of all the parameters in one objective function instead y_1^* we will consider the modified parameter $y_1 = 1 / y_1^*$. All parameters will correspond to the basic behavior of the objective function "less is better".

III. Borders calculation of optimization parameters changes. In Table 1 the relationship $A = P_s / P_n$ for 12 GHz frequency range and for 18 GHz frequency range is shown.

Tables marked border, where the ratio $A = P_s / P_n$ is less acceptable.

Table 1.

f_c = 12 GHz, FEC = 5/6 $P^{tr.}_{transm}$ = 20 W, $\Delta f^{tr.}$ = 100 MHz		A2 Ø	K_m=1	K_m=2	K_m=4
at output of A2 P_c [W] for one TV-program		1 m	$6.35 \cdot 10^{-14}$	$3.17 \cdot 10^{-14}$	$15.5 \cdot 10^{-15}$
		2.7 m	$3.37 \cdot 10^{-12}$	$1.6 \cdot 10^{-12}$	$8.4 \cdot 10^{-13}$
Δf^{n}_{OFDM}		AA ES P_n [W]	350 MHz; $1.99 \cdot 10^{-12}$		11 MHz; $6.25 \cdot 10^{-14}$
			100 MHz; $5.69 \cdot 10^{-13}$		4 MHz; $2.27 \cdot 10^{-14}$
			20 MHz; $1.14 \cdot 10^{-13}$		
ØA2 1m	350 MHz	$10\lg A$, $A = \frac{P_s}{P_n}$ [dB]			
	100 MHz				
	20 MHz				
	11 MHz		0	-3,0	-6,2
	4 MHz		4,47	1,43	-1,67
ØA2 2.7m	350 MHz	$10\lg A$, $A = \frac{P_s}{P_n}$ [dB]	-0,76	-3,77	6,23
	100 MHz		7,7	4,7	1,5
	20 MHz		14,6	11,7	8,7
	11 MHz		17,3	14,4	11,3
	4 MHz		21,7	18,7	15,7

The parameters of 5 types of antennas, 4 types of modulation, MPEG2 and MPEG4 were used for calculations.

К=1 (ФМ-1); К=2 (QPSK); К=3 (ФМ-8);

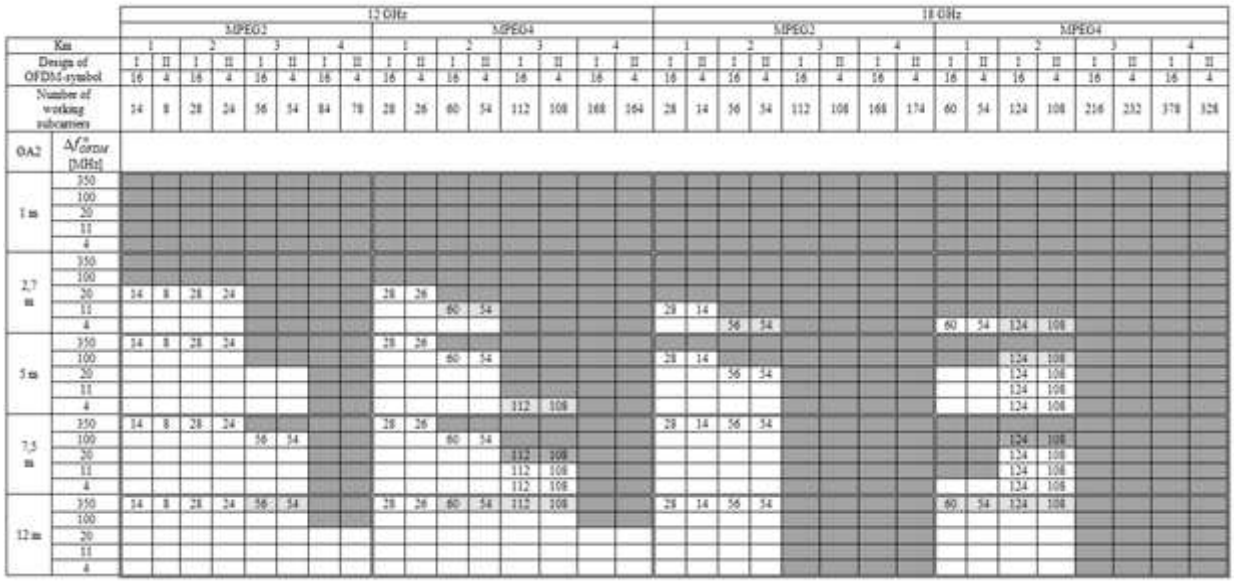
К=4 (QAM-16); К=5 (QAM-32); К=6 (QAM-64) (Fig. 2).

Table 1 (12 GHz) presents the data for calculating the ration $10 \cdot \lg(P_s / P_n)\,[dB] = F(\Delta f^{n}_{OFDM})$ at Δf^{n}_{OFDM} = 350 MHz, 100 MHz, 20 MHz, 11 MHz and 4 MHz for Earth stations receive signals, which have different antennas at the input of A2.

Promising results showed earth station with antenna a mirror diameter equal

to A2 7.5 m and 5.0 m. According to Table 2 with these data it is enough to have 4 transponder, at that in both bands at the operating frequency band of noise is equal not to 20 MHz, but to 100 MHz.

Table 2. Parameters of 24 the most promising earth reception stations of the satellite signal in the distribution network of television programs.



In this sce nario, the antenna A2 with a mirror diameter of 12 meters is unnecessary luxury, that will change a little in the final result, in addition, that this station will be considerably more expensive than 260000 $ instead of 90000 $ in the range of 12 GHz and a 500000 $ instead of 150000 $ in the range of 18 GHz [2].

Conclusion

1. Table 1 shows the main parameters of earth stations reception satellite signals, OFDM-symbols and provides the data structure of how many subcarriers may be working in a transponder with a view to ensuring the reception quality with the bit error probability $\leq 10^{-5}$.
2. Since the most expensive antenna ES (A2), selecting them means to provide the most secure network operation success.

References

1. Kalnibolotsky Y.M., Sunduchkov K.S., Solodovnik A.I. Automated design of electronic circuits // Technology, 1987 ill. – Bibliogr.: pp.291-299.
2. A.M.Bonch-Bruevich, V.L.Bykov, L.Y.Kantor and others Satellite communications systems // Radio and Communications, 1992 .; ed. L.Y.Kantor: Textbook for High Schools. – 224 p.: pp.209.

УДК 621.396.43

DIGITAL RADIO SIGNALS TRANSMISSION OF DVB-T AND DVB-T2 STANDARDS BY USING TERAHERTZ FREQUENCY - BAND RADIO CHANNEL.

Drobina O.S., Avdeyenko G.L., Naritnik T.M., Naboka B.Y.
Institute of Telecommunication Systems NTUU "KPI"
E-mail: oleg.drobina.kpi@gmail.com

Передача сигналів ЦТБ стандартів DVB-T та DVB-T2 по радіорелейній лінії терагерцового діапазону

Робота відображає результати експерименту з передачі радіосигналів цифрового телебачення стандартів DVB-T та DVB-T2 через макет одноінтервальної симплексної радіорелейної лінією терагерцового діапазону хвиль. Отримані дані дозволяють зробити висновки з можливості використання наявного макету радіорелейної лінії терагерцового діапазону для якісної передачі та прийому сигналів з COFDM модуляцією.

Introduction.

Terahertz waves («T-rays») are electromagnetic waves in a frequency band of 100 – 3000 GHz. Compared to the relatively well studied and technically secured microwave, optical and X-ray, advances in research and application of terahertz radiation so far are limited and are likely to demonstration level, despite the extremely high possibility of their technical and biomedical use, for example in infrared astronomy and oncology [1].

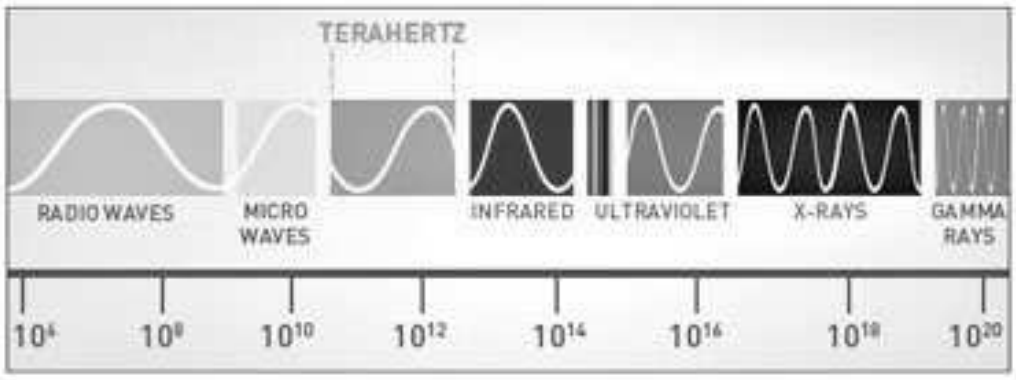


Fig.1 Place of terahertz frequency ratio in electromagnetic spectrum.

Main part.

There is a research on the demonstrative level of the possibility of transmission of signals of DVB-T and DVB-T2 standards by using radio-relay line (RRL) of terahertz frequency band (THz) in this work. Let us take a look at the principal scheme (Fig.2). It is a RRL of THz where the transmission of signal happens on the frequency of 130 GHz. At the input of transmission and the output of receiving parts, analyzers are placed for measuring of parameters of the signal that is being transmitted and the signal that is being received. Also, receiver and

TV are placed on the output for checking of the possibility of demodulation of the transmitted signal and getting of TV image and sound. The task of the experiments is in alternately transmission of DVB-T and DVB-T2 signals through the RRL and measuring of their parameters for getting practical results and rating of the usefulness of using of «T-rays» in practice.

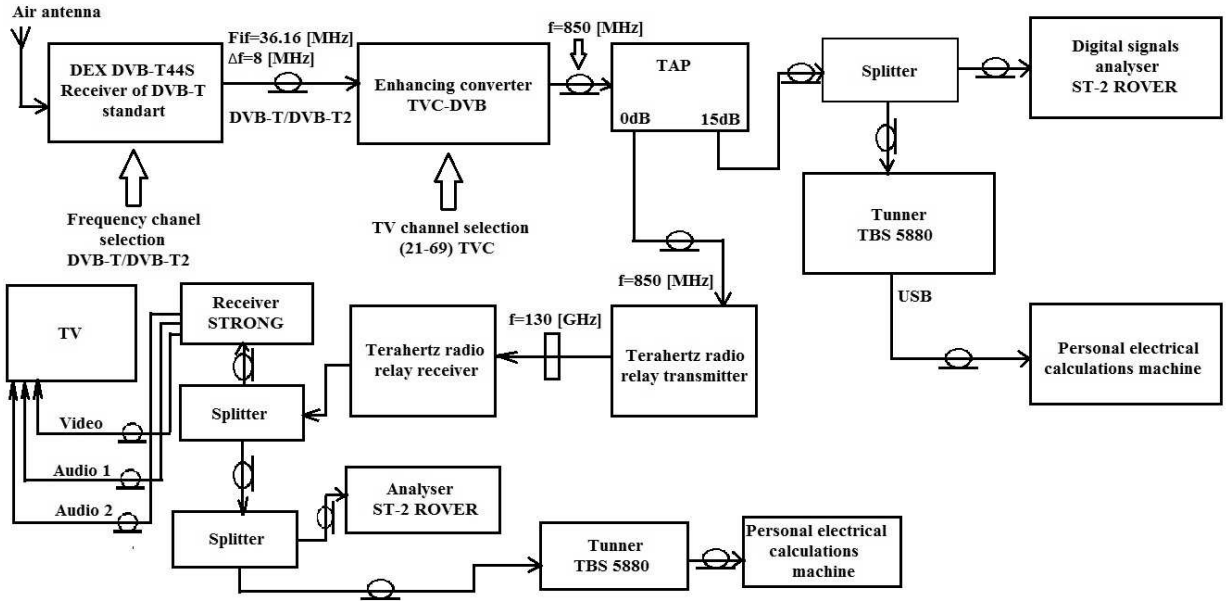


Fig.2 Principal scheme for transmission of signals of DVB-T and DVB-T2 standards through RRL of THz research

Experiment №1. Transmission of digital TV signal of DVB-T standard through RRL of THz.

The source of DVB-T signal is a digital multiplex with a frequency of 650 MHz. Signal passed the terahertz path after pretreatment and there was a high quality image on the TV receiver. The results of parameters measurements of the signal with the help of ST-2 ROVER analyzer are shown in Table 1.

Table 1. DVB-T signal research results

Digital TV transmission of signals by RRL THz research		
DVB-T		
Parameters	Input value	Output value
N.MAR [dB]	5	5
aBER	$5 * 10^{-7} - 7 * 10^{-7}$	$< 10^{-8}$
bBER	$2 * 10^{-3}$	$3 * 10^{-3}$
SNR [dB]	29	29
MER [dB]	24,6	24
PWR [dBm]	-35,8	-45,3
CARR.	8KDTB-T	8KDVB-T
QLTY	MARG	MARG

Table 2. DVB-T2 signal research results

Digital TV transmission of signals by RRL THz research		
DVB-T2		
Parameters	Input value	Output value
N.MAR [dB]	6	7
QLTY	PASS	PASS
C/N [dB]	30	31
FLAT [dB]	6	7
BER	$1 * 10^{-7}$	$1 * 10^{-7}$
MODE	QAM256	QAM256
PWR	-31,6	-41,2

Experiment №2. Transmission of digital TV signal of DVB-T2 standard through RRL of THz.

The source of DVB-T2 signal is a digital multiplex with a frequency of 514 MHz. Signal was being passed through the THz path, like in the previous experiment, and at the output of RRL of THz with the help of receiver we have got

a high quality image and sound on the TV. The data, which obtained at the input and output of RRL of THz using ST-2 ROVER emulation mode, are presented in Table 2.

Also, the received signal constellations by using TBS 5880 receiver of CrazyScan program, are presented on fig.3 – fig.6.

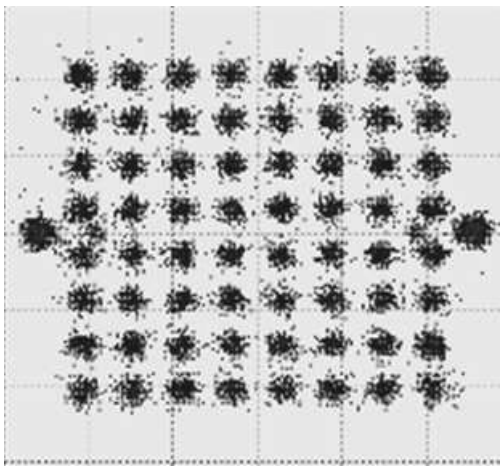


Fig.3 DVB-T signal at the input of RRL.

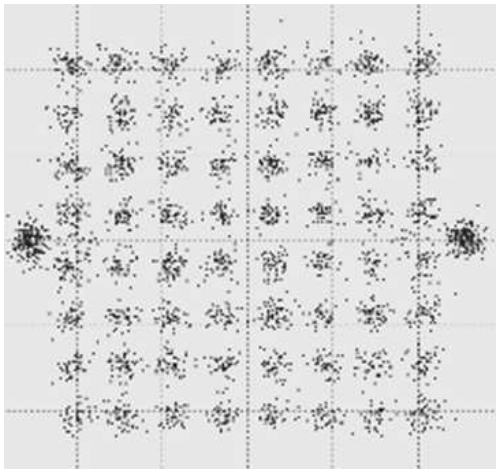


Fig.4 DVB-T signal at the output of RRL.

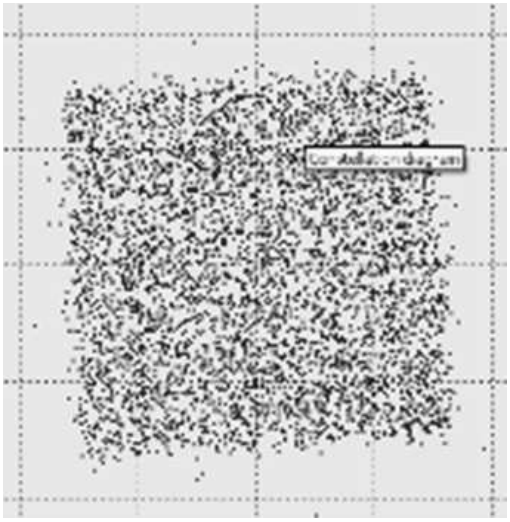


Fig.5 DVB-T2 signal at the input of RRL.

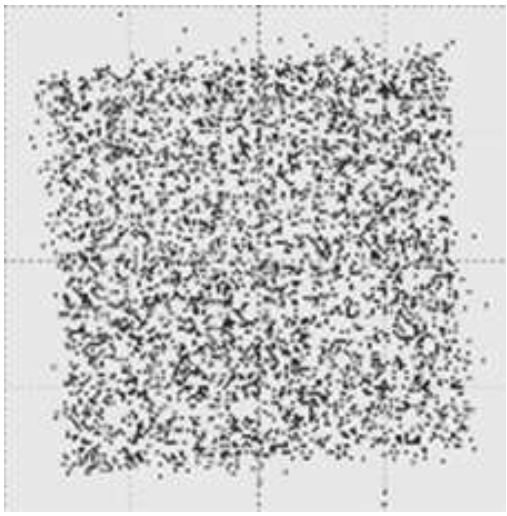


Fig.6 DVB-T2 signal at the output of RRL.

Conclusions.

So, as the results of the experiment show, high quality signals DVB-T/DVB-T2 were received with minimal distortion and low probability of error. It proves the possibility to use RRL of THz for transmission of radio-signals with COFDM modulation, which are DVB-T and DVB-T2 signals.

References

1. Кравчук С.О. Телекомунікаційні системи терагерцового діапазону. Монографія.//Житомир.: ФОП «Євенок О.О.».--2014.-394с. Кравчук С.О., Наритник Т.М.

UDC 621.39

SAAS VIRTUALIZATION METHOD AND ITS APPLICATION

Chernyavsky A. A., Pilipenko A. A.
Institute of Telecommunication Systems NTUU "KPI"
E-mail: ruskc2beat@gmail.com, lex.pilipenko@gmail.com

Метод виртуализации SaaS и его применение

В работе предлагается метод построения информационной системы для компании, которая нуждается в сервисах облачного вычисления. Этот метод основывается на объединении преимуществ облачных технологий, которые используют телекоммуникационные операторы, и технологии SaaS. Этот метод комбинирует базовую систему услуг SaaS и магистральную систему, расположенную на производственной площадке, с VPN в замкнутой области сети.

Introduction. Nowadays the Internet is used for business by different companies. Not only telecom companies provide information business. There are also cloud computing services and SaaS vendors (companies, that offer SaaS services). Telecom operators are seeking the safety of communication offering their services. SaaS vendors are trying to provide more economical and convenient service as well.

In this paper we propose a method of configuring an information system for a company that needs cloud computing services. The main idea is to optimize the advantage of cloud computing service provided by telecom operators and SaaS vendors.

We have identified the difference in policy and issue of telecom operator, SaaS vendor and client company. It is shown in Table 1.

Table-1 Policy and issue

	Telecom operator	**SaaS vendor**	**Client companies**
System policy	Provides overall network services	Constructs own SaaS system	Construct a backbone system
Business policy	Provides End-to-End network services Pursuing the security of communication	Pursuing economy Pursuing convenience Encloses a lot of companies with needs	Fast access to information Updating of business process Low cost
Issue	Paying attention to network service	Forcing security of communication	Functionality Enhancement of systems

Main part. Two systems existing in different network spaces work separately and the stored information cannot cooperate. It means that the SaaS base system and on-premise backbone system existing in different network spaces operate independently and the information cannot be shared.

So we propose “SaaS virtualization method” (Fig.1). The main idea of this method is to connect the SaaS base system and the on-premise VPN backbone system of closed area network. It will be possible to connect the SaaS base service system assigned to each client company existing externally to the on-premise backbone system existing internally. That is, the external SaaS base system and the internal backbone system are combined together by virtualization.

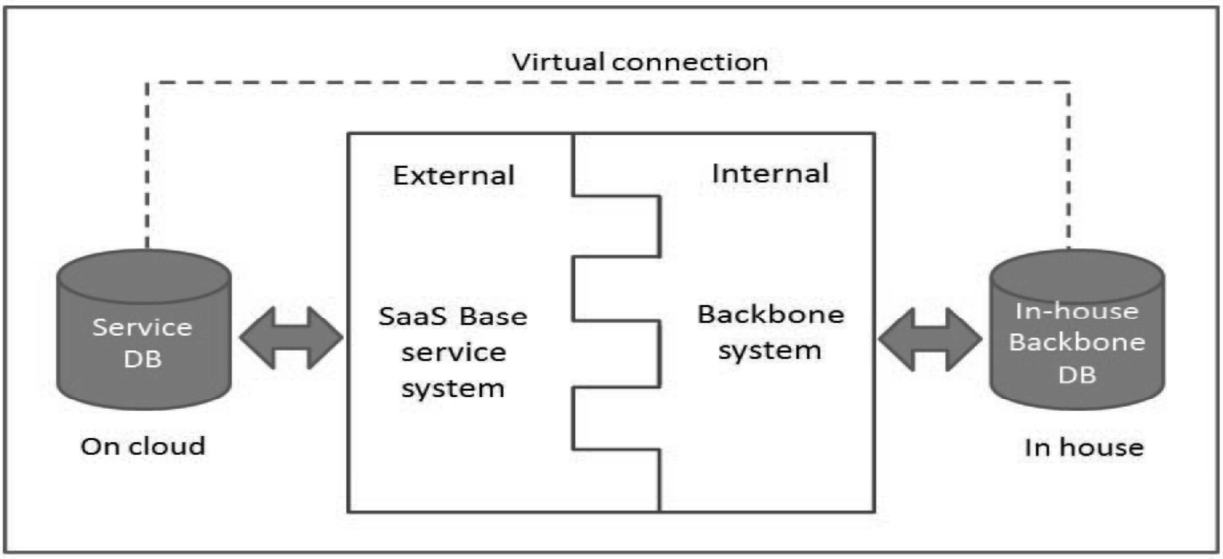


Fig.1 SaaS Virtualization Method

Implementation. To realize the system we described earlier we need the cloud service that enables client company to utilize SaaS service assigned through secure VPN network. It can be implemented by constructing the commercial application type cloud service on the SaaS basic service. This service realizes secure connection by connecting three different network spaces: on-premise backbone system of client company, the network space of VPN and the network space of gateway that combines two former network spaces. So the external SaaS base system and the internal backbone system are securely combined together by connecting these three different networks by virtualization. As a result, a company can utilize SaaS service assigned by cloud service company as on-premises.

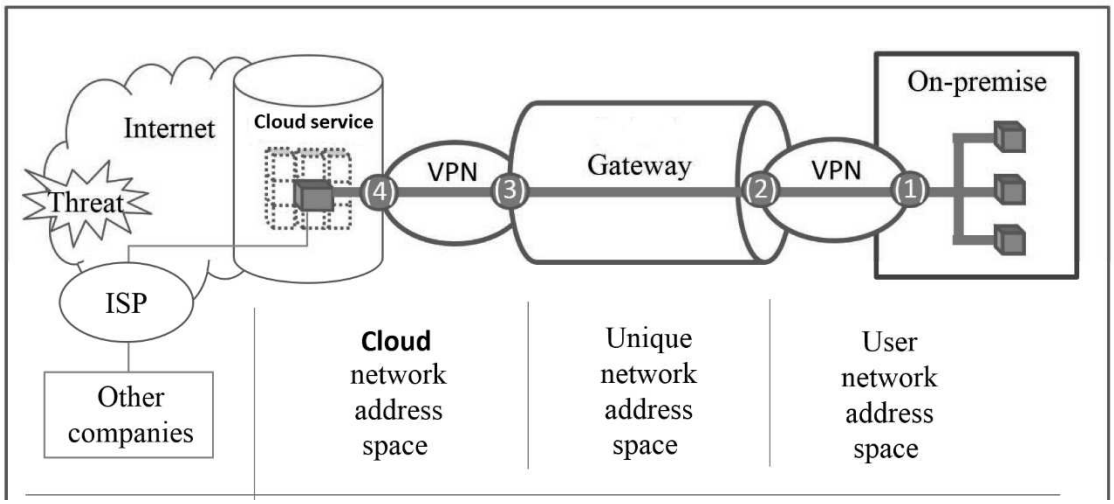


Fig.2 Construction of secure connection

We will describe in details the communication of this model. The IP packet sent from the on-premise system has the source IP address (1), and the destination

IP address (2) of the on-premise side of gateway system. The port number is 1000. When the IP packet reaches the gateway system, the source IP address is rewritten from (1) to (3) of cloud service side, the destination IP address is rewritten from (2) to (4) of cloud service and the source port number is rewritten from 1000 to 3000. Cloud service system receives the rewritten IP packet and replies the IP packet to the gateway system. The IP packet sent from the cloud service system is the source IP address (4) and the destination IP address (3) of cloud service. When the IP packet reaches the gateway system, it is being transferred to the on-premise system with rewritten from (4) to (2) source IP address and rewritten from (3) to (1) destination IP address. The port number is rewritten from 3000 to 1000. The on-premise system receives the reply packet from the cloud service system.

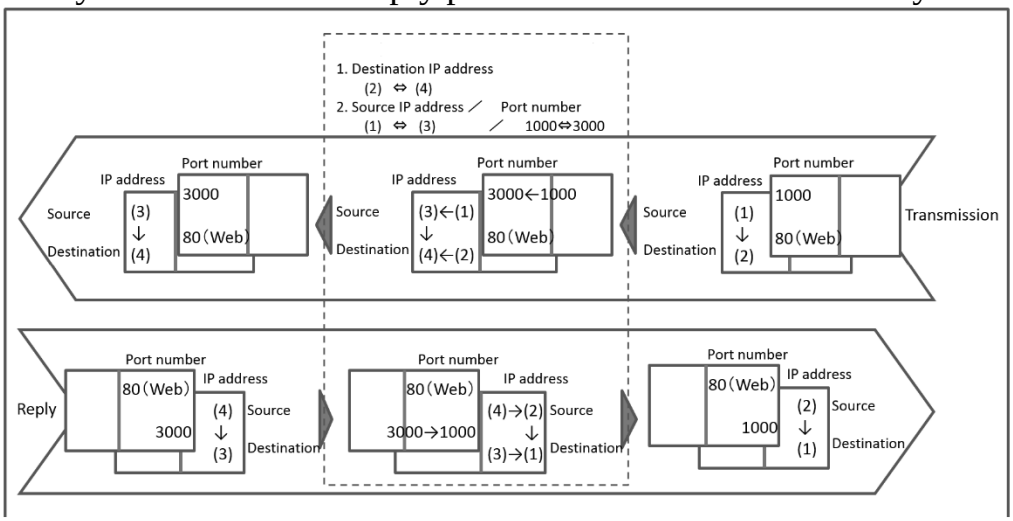


Fig. 3 Details of the communication.

Conclusion. As a result, the company will be able to utilize resources given by using cloud services, especially using SaaS model, therefore dramatically increasing services infrastructure. Moreover, the use of virtualization technologies will provide high mobility of software solutions which are needed to maintain redundant IT environment. Also, the use of VPN solution will be brought to solve security issues while exchanging data between company's network and cloud.

References

1. Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia 2009 "Above the Clouds: A Berkeley View of Cloud Computing" UC Berkeley Reliable Adaptive Distributed Systems Laboratory – Available at: http://radlab.cs.berkeley.edu/.
2. Kenichi Miyazawa, "Increased use of service, information and network in industrial society" Hitotsubashi selection of treaties, Vol.97, No. 5.
3. Heihachiro Yamaguchi, Masayuki Ida "SaaS Virtualization Method and Its Application".

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ
НДІ ТЕЛЕКОМУНІКАЦІЙ

Восьма Міжнародна науково-технічна конференція студентів та аспірантів «ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА СИСТЕМ»

Присвячено Дню науки та Всесвітньому Дню телекомунікацій

19–22 квітня 2016 року

Тези конференції

м. Київ

ПРОГРАМНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ ПРІТС-2016

(в дужках вказано номери напрямків, що формуються членами наглядового комітету)

Співголови конференції:

ІЛЬЧЕНКО М.Ю. – проректор з наукової роботи Національного технічного університету України "Київський політехнічний інститут", академік НАНУ, д.т.н., професор;

ЯКОРНОВ Є.А. – заступник директора інституту телекомунікаційних систем НТУУ «КПІ», к.т.н., професор;

ЛАЗАРЕНКО О.П. – голова студентської ради інституту телекомунікаційних систем НТУУ «КПІ».

Члени наглядового комітету:

УРИВСЬКИЙ Л.О. - д.т.н., проф., НТУУ «КПІ», Київ, (1, 9), e-mail: leonid_uic@ukr.net;
МАКСИМОВ В.В. - к.т.н., доц. НТУУ «КПІ», Київ, (1), e-mail: maksimov46@ukr.net;
МОШИНСЬКА А.В. - к.т.н., доц., НТУУ «КПІ», Київ, (1), e-mail: moshinskaya@mail.ru;
ТРУБІН О.О. - д.т.н., проф., НТУУ «КПІ», Київ, (2), e-mail: atrubin@ukrpost.ne;
ШЕЛКОВНІКОВ Б.М. - к.т.н., доц., НТУУ «КПІ», Київ, (2), e-mail: bshelk@gmail.com;
ТРУБАРОВ І.В. – к.т.н., ст. викладач, НТУУ «КПІ», Київ, (2), trubarov_igor@mail.ru;
РОМАНОВ О.І. - д.т.н., проф., НТУУ «КПІ», Київ, (3), e-mail: a_i_romanov@mail.ru;
КАТОК В.Б. - к.т.н., проф., ПАТ «Укртелеком», (3), Київ, vkatok@ ukrtelecom.net;
НАРИТНІК Т.М. - к.т.н., проф., НТУУ «КПІ», (4), Київ, e-mail: director@mitris.com;
КРАВЧУК С.О. - д.т.н., проф., НТУУ «КПІ», Київ, (4), e-mail: sakravchuk@ukr.net
МІНОЧКІН Д.А. - к.т.н., ст. викладач, НТУУ «КПІ», Київ, (4), dminochkin@mail.ru
ГЛОБА Л.С. - д.т.н., проф., НТУУ «КПІ», Київ, (5), e-mail: lgloba@hotmail.com;
СКУЛИШ М.А. - к.т.н., доц., НТУУ «КПІ», Київ, (5), e-mail: mskulysh@gmail.com;
ПРАВИЛО В.В. - к.т.н., доц., НТУУ «КПІ», Київ, (5), e-mail: valeriy_pravilo@ukr.net;
ЛИСЕНКО О.І. - д.т.н., проф., НТУУ «КПІ», Київ, (6), a_i_lysenko@voliacable.com;
ЯВІСЯ В.С. - к.т.н., доц., НТУУ «КПІ», Київ, (8), e-mail: yavisya@bigmirinet;
ЛІПАТОВ А.О. - к.т.н., проф., НТУУ «КПІ», Київ, (8), e-mail: anlip27@ukr.net;
БУНІН С.Г. - д.т.н., проф., НТУУ «КПІ», Київ, (9), e-mail: sgbunin@ukr.net.

Члени програмного комітету:

1. Бунін С.Г., д.т.н., проф., ІТС
2. Уривський Л.О., д.т.н., проф., ІТС
3. Мошинська А.В., к.т.н., доц., ІТС
4. Трубаров І.В., к.т.н., ст. викладач, ІТС
5. Романов О.І., д.т.н., проф., ІТС
6. Міночкін Д.А., к.т.н., ст. викладач, ІТС
7. Скулиш М.А., к.т.н., доц., ІТС
8. Валуйський С.В., к.т.н., ст. викладач, ІТС
9. Ліпатов А.О., к.т.н., проф., ІТС
10. Синепольський Ю.В., аспірант ІТС
11. Кулік О.В., студ. ІТС
12. Верес Л.А., студ. ІТС
13. Жогов Р.Ю., студ. ІТС.

Засідання 1.

METHODS OF GENERATING, DISTRIBUTING INFORMATIONAL-PSYCHOLOGICAL INFLUENCE IN THE TELECOMMUNICATION SYSTEMS

Ahtyrtseva V.S.
Scientific adviser: Dr. of Techn. Sci. Hryshchuk R.V.
Zhytomyr Military Institute after S. P. Korolyov, 17 Lisova st., v.Novoivnycja, Andrushivka district, Zhytomyr region, 13419,Ukraine
E-mail: perri92@i.ua

For the generation of content with hidden information-psychological influence are encouraged to use informational masking effects in habitual for the Internet user formats, i.e. audio and video files, JPG files , in executable files. To hide the essence of the destructive informational influence to impede signature analysis using the code transformation (obfuscation of source code) and steganography methods. For information and psychological impact of using technology type "25 frame".

For content distribution, you should use a botnet for social networks, since it is possible to immediately capture a large number of audiences especially the youth, more exposed to information-psychological influence. The use of these technologies allows to create information-psychological weapon for waging war in cyberspace.

МЕТОДИ ГЕНЕРУВАННЯ, ПОШИРЕННЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ВПЛИВІВ У ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Ахтирцева В.С.
Науковий керівник: д.т.н. Грищук Р.В.
Житомирський військовий інститут імені С. П. Корольова, вул. Лісова 17, с. Новоівницьке, Андрушівський район, Житомирська область, 13419,Україна
E-mail: perri92@i.ua

Для генерації контенту зі скритим інформаційно-психологічним впливом пропонується використовувати маскування інформаційного впливу у звичних для користувача мережі Інтернет форматах, тобто в аудіо та відеофайлах, в зображеннях JPG, у файлах, що виконуються. Щоб приховати суть руйнівного інформаційного впливу, для утруднення сигнатурного аналізу використовують перетворення коду (обфускація вихідних кодів) та методи стеганографії. Для інформаційно-психологічного впливу використовують технології типу вбудовування «25 кадру».

Для поширення контенту слід використовувати бот-мережу для соціальних мереж, оскільки є можливість захопити одразу велику кількість аудиторії та особливо молодь, що найбільше піддається інформаційно-психологічному впливу. Використання цих технологій дає можливість створити інформаційно-психологічну зброю для ведення війни у кіберпросторі.

IMPLEMENTATION CONFERENCE AUDIO SERVER BASED IP PBX FREESWITCH

Mazharenko E.V.
Scientific adviser: **Maksimov V.V.**
Institute of Telecommunication Systems NTU "KPI", Ukraine
E-mail: kyiv12@bigmir.net

IP PBX FreeSWITCH indicated support for access to multiple parties conference communications. In the default configuration set up certain kinds of conferences which users can use immediately after installing the switch. To test the conference will take at least 2 phones and other user session, which helps to ensure proper operation of the conference room. In fixed softswitches default also necessary to establish sound and music files.

РЕАЛІЗАЦІЯ СЕРВЕРУ АУДІО КОНФЕРЕНЦІЇ НА БАЗІ IP PBX FREESWITCH

Мажаренко Є.В.
Науковий керівник: **Максимов В.В.**
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: kyiv12@bigmir.net

IP PBX FreeSWITCH відзначається підтримкою доступу до конференції кільком сторонам зв’язку. У конфігурації за замовчуванням налаштовані певні типи конференцій які користувачі можуть використовувати відразу після встановлення програмного комутатору. Для тестування роботи конференції знадобиться принаймні 2 телефони для сеансу та інший користувач, який допоможе переконатись в правильній роботі конференц-кімнати. Крім встановленого програмного комутатору за замовчуванням також необхідне встановлення звукових та музичних файлів.

DATA PROTECTION IN VIRTUAL PRIVATE NETWORK

Saienko B. V.
Scientific adviser: Professor **Romanov A.I.**
Institute of Telecommunication Systems NTUU "KPI", Ukraine
E-mail: saienko.bohdan@gmail.com

Big corporations consist of some remote branches among which reliable, secure interaction using public channels of Internet network must be organized. This problem can be solved by using different kinds of Virtual Private Network. The use of integral cryptographic methods in network equipment allows encrypting traffic with durability guarantee. In the network laboratory of Telecommunications Department a model of real part of VPN network, on which researches are made and ways of optimization are developed, has been created.

ЗАЩИТА ИНФОРМАЦИИ В VIRTUAL PRIVATE NETWORK

Саенко Б. В.
Научный руководитель: д.т.н, профессор **Романов А. И.**
Институт телекоммуникационных систем НТУУ «КПИ», Украина
E-mail: saienko.bohdan@gmail.com

Крупные корпорации состоят из нескольких удаленных филиалов, между которыми должно быть организовано надежное, защищенное взаимодействие с использованием общедоступных каналов Интернет сети. Такую задачу можно решить путем применения различных видов Virtual Private Network. Использование встроенных в аппаратуру сетей средств криптографической защиты, позволяет шифровать трафик с гарантированной стойкостью. В лаборатории кафедры телекоммуникаций создан макет реального участка сети VPN, на котором производятся исследования и разрабатываются предложения по оптимизации.

POSSIBLE METHODS TO MAINTAIN RELIABILITY OF COMMUNICATION IN THE 802.11N PROTOCOL

Shevchenko M.V.
Scientific adviser: Dr.of Sc. Uryvsky L.A.
Institute of Telecommunication Systems NTUU "KPI"
E-mail: marshelka@meta.ua

One of the main tasks of telecommunication systems is the transmission of a predetermined amount of information, the solution of which depends on achievement of specified reliability. There are several methods of communicating reliability in the 802.11n protocol. The most famous among them: changing the multiplicity of manipulation, improvement reliability due to OFMD by selective amplification, the transition to more powerful codes in coding. In this article is considered the maintain algorithms of reliability by the methods described earlier.

ВОЗМОЖНЫЕ МЕТОДЫ ПОДДЕРЖАНИЯ ДОСТОВЕРНОСТИ СВЯЗИ В ПРОТОКОЛЕ 802.11N

Шевченко М.В.
Научный руководитель: д.т.н., проф. Урывский Л.А.
Институт телекоммуникационных систем НТУУ «КПИ», Украина
E-mail: marshelka@meta.ua

Одной из главных задач телекоммуникационных систем является передача заданного объема информации, решение которой зависит от достижения заданной достоверности. Существует несколько методов поддержания достоверности связи в протоколе 802.11n. Самые известные среди них: изменение кратности манипуляции, улучшение достоверности за счёт OFMD методом селективного усиления, переход к более мощным кодам в кодировании. В данной статье рассматриваются алгоритмы поддержания достоверности описанными методами.

DELIVERY OF SIGNALS OVER SATELLITE RADIO CHANNELS IN A HETEROGENEOUS DISTRIBUTION NETWORK

Iryna Tymchenko
Scientific adviser: Konstantin Sunduchkov
Institute of Telecommunication Systems, NTUU "KPI", Ukraine
E-mail: iratim4enko@gmail.com

This paper provides such methods of controlling of the delivery of signals to base stations, as alignment electrical pathways, the use of delay lines, the regulation of the location of base stations.

ДОСТАВКА СИГНАЛОВ УСЛУГ ПО СПУТНИКОВОМУ РАДИОКАНАЛУ В ГЕТЕРОГЕННОЙ РАСПРЕДЕЛИТЕЛЬНОЙ СЕТИ

Тимченко И.О.
Научный руководитель: Сундучков К.С.
Институт телекоммуникационных систем НТУУ «КПИ», Украина
E-mail: iratim4enko@gmail.com

В данной работе предложены такие способы регулирования доставки сигналов к базовым станциям, как выравнивание электрических путей, использование линий задержки, регулирование местоположения базовых станций.

ARCHITECT'S GUIDE: IOT SECURITY

Kuzianin A.S.
Scientific adviser: Ph. D. **Globa L.S.**
Institute of Telecommunication Systems NTUU "KPI", Ukraine
E-mail: sasha.kuzianin@gmail.com

The article is based on the description of steps to optimize and improve IoT (Internet of Things) security. Basic security issues that arise in the network construction and the basic methods of overcoming them.

АРХИТЕКТУРА БЕЗОПАСНОСТИ ТЕХНОЛОГИИ INTERNET OF THINGS, IOT

Кузянин А.С.
Научный руководитель: д.т.н., проф. **Глоба Л.С.**
Институт телекоммуникационных систем НТУУ «КПИ», Украина
E-mail: sasha.kuzianin@gmail.com

Статья основана на описании шагов для оптимизации и повышения IoT (Internet of Things). Основные проблемы безопасности, которые возникают при строительстве сети и основные методы их преодоления.

INTERRELATION OF RESOURCES OF THE MULTISERVICE COMMUNICATION NETWORK AND ITS INFORMATION OPPORTUNITIES

Bazhenov P. O.
Scientific adviser: Ph.D., docent **Moshynskaya A. V.**
Institute of Telecommunication Systems NTUU «KPI»
E-mail: pbazhenovo@gmail.com

In paper the analysis of interrelation of multiservice network resources and its information opportunities with the subsequent their assessment according to-level architecture of a multiservice network. It will allow to estimate information opportunities of a multiservice network on the basis of the available resource and to define ways achievement transfer of the maximum quantity of information in borders of the provided resource.

ВЗАИМОСВЯЗЬ РЕСУРСОВ МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ И ЕЕ ИНФОРМАЦИОННЫХ ВОЗМОЖНОСТЕЙ

Баженов П. О.
Научный руководитель: к.т.н., доцент **Мошинская А. В.**
Институт телекоммуникационных систем НТУУ «КПИ»
E-mail: pbazhenovo@gmail.com

В работе предлагается анализ взаимосвязи ресурсов мультисервисной сети и ее информационных возможностей с последующей их оценкой согласно уровневой архитектуры мультисервисной сети. Это позволит оценить информационные возможности мультисервисной сети на основе имеющегося ресурса и определить способы достижения передачи максимального количества информации в границах предоставленного ресурса.

PROTECTING THE NETWORK FROM OVERLOADING BY USING THE MECHANISM OF EXPLICIT CONGESTION NOTIFICATION (ECN).

Kuklina A. S.
Scientific adviser: Ph.D. **Romanov A. I.**
Institute of telecommunication systems NTUU "KPI"
E-mail: kuklina_anna1995@mail.ru

Telecommunication networks are prone to overloading caused by increasing traffic intensity. To set the operation of the network in normal mode, various methods can be used, in particular Explicit Congestion Notification (ECN) that allows to detect network congestion occurs solve the problem without dropping packets. In the laboratory of the Department of Telecommunications Network a display stand of the network was created and has been used for researching methods of preventing congestion using ECN.

ИСПОЛЬЗОВАНИЕ МЕХАНИЗМА EXPLICIT CONGESTION NOTIFICATION (ECN) ДЛЯ ЗАЩИТЫ СЕТЕЙ ОТ ПЕРЕГРУЗКИ

Куклина А. С.
Научный руководитель д.т.н. **Романов А.И.**
Институт телекоммуникационных систем НТУУ «КПИ», Украина
E-mail: kuklina_anna1995@mail.ru

Телекоммуникационные сети подвержены перегрузкам в следствии увеличения интенсивности трафика. Для приведения процесса функционирования сети в нормальный режим, могут быть использованы различные методы, в частности Explicit Congestion Notification (ECN), что позволяет узнавать о возникновении затора на маршруте и привести сеть в нормальный режим работы без отбрасывания пакетов. В лаборатории кафедры Телекоммуникаций создан стенд участка сети, на котором проводятся исследования борьбы с перегрузками с использованием ECN.

INTERNET OF THINGS IN MODERN TELECOMMUNICATION NETWORKS

Mieliekhova M.O., Bilan A.M.
Scientific adviser: **Kravchuk S.O.**
Institute of telecommunications systems. NTUU "KPI", Ukraine
E-mail: maria.melekhova@gmail.com, bilan-n@ukr.net

We consider the concept of the "Internet of things", which combines technologies such as cloud computing, analytics, big data, mobility, accessibility, means of collaboration and security equipment, and its implementation using hardware Arduino. Galileo - the first Arduino-compatible microcomputer on the platform Intel. The use of technology in projects "smart city" - Barcelona, Lyon, Paris, Nice, Strasbourg.

ІНТЕРНЕТ РЕЧЕЙ В СУЧАСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Мєлєхова М.О., Білан А.М.
Науковий керівник: **Кравчук С.О.**
Інститут телекоммуційних систем. НТУУ "КПІ", Україна
E-mail: maria.melekhova@gmail.com, bilan-n@ukr.net

Розглянуто концепцію "Інтернет речей", яка поєднує в собі технології, такі як хмарні обчислення, аналітика, великі данні, мобільність, доступність, засоби забезпечення колективної роботи і безпеки обладнання, та її реалізація за допомогою апаратних засобів Arduino. Galileo - перший Arduino-сумісний мікрокомп'ютер на платформі Intel. Застосування технологій у проектах "інтелектуальне місто" - Барселона, Ліон, Париж, Ніцца, Страсбург.

NODE.JS FOR DEVELOPING MODERN REAL-TIME SERVICES

Ostapenko S.O.
Scientific adviser: **Prischepa T.O.**
Institute of Telecommunication Systems NTU "KPI", Ukraine
E-mail: serg.ostapenko94@gmail.com

Analyzed the basic features of the Node.js platform. The comparison in the classical model and asynchronous I / O data. Considered the basic application platform usage. Identified the basic advantages and disadvantages of modern technology to others.

NODE.JS ДЛЯ РОЗРОБКИ СУЧАСНИХ СЕРВІСІВ ЯКІ ПРАЦЮЮТЬ В РЕЖИМІ РЕАЛЬНОГО ЧАСУ

Остапенко С.О.
Науковий керівник: **Прищепа Т.О.**
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: serg.ostapenko94@gmail.com

Проаналізовано основні особливості роботи платформи Node.js. Проведено порівняння в роботі класичної та асинхронної моделі вводу / виводу даних. Розглянуті основні місця застосування платформи. Визначені головні переваги та недоліки даної сучасної технології перед іншими.

IMPLEMENTATION OF VIDEO CONFERENCE BASED ON IP PBX ASTERISK

Pobuta O.V.
Scientific adviser: **Maksimov V.V.**
Institute of Telecommunication Systems NTU "KPI", Ukraine
E-mail: oleg.pobuta@gmail.com

New versions of IP PBX ASTERISK can support video conferencing. They implemented through application confbridge. Appendix ConfBridge has four interior concepts: Conference Number; Bridge Profile; User Profile; Conference Menu.

Sections and menus of ConfBridge are described in the configuration file confbridge.conf, which is usually located in /etc/asterisk/confbridge.conf.

This service were configured on the equipment of department of telecommunication systems ITS NTUU "KPI" and is aimed at improving the department and provide a basis for further research technologies.

РЕАЛІЗАЦІЯ ФУНКЦІЇ ВІДЕО КОНФЕРЕНЦІЇ НА БАЗІ IP PBX ASTERISK

Побута О.В.
Науковий керівник: **Максимов В.В.**
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: oleg.pobuta@gmail.com

Нові версії IP PBX ASTERISK відзначаються підтримкою відео конференцій. Вони реалізуються за допомогою додатку *confbridge.* Додаток ConfBridge має чотири внутрішні концепції: Номер конференції; Профіль конференції; Профіль користувача; Меню конференції.

Профілі й меню програми ConfBridge описуються у файлі конфігурації *confbridge.conf*, який зазвичай знаходитися в */etc/asterisk/confbridge.conf*.

Даний функціонал було налаштовано на обладнанні кафедри телекомунікаційних систем ІТС НТУУ «КПІ» і спрямовано на поліпшення роботи кафедри і створення бази для подальших досліджень технології.

VIDEO TELEMETRY SYSTEM FOR GEOSTATIONARY TELECOMMUNICATION SATELLITE

Paradovskyi A. A.
Scientific adviser: d.t.s., Professor. **Romanov A. I.**
Scientific consultant: **Pyzyk D. L.**
Institute of telecommunication systems NTUU "KPI"
E-mail: aparadovsky@gmail.com

The rapid development of information technology tools and tendency to space segment complications dictate the need for new systems of digital telemetry information formation. These systems are used for data compilation and transmission to Earth about the status of the spacecraft and its subsystems. Installing cameras in the geostationary satellite platform will expand the functionality of existing telecontrol systems and give the opportunity to track the status of the spacecraft more effective.

СИСТЕМА ВИДЕОТЕЛЕМЕТРИИ ДЛЯ ГЕОСТАЦИОНАРНОГО ТЕЛЕКОММУНИКАЦИОННОГО СПУТНИКА

Парадовский А. А.
Научный руководитель: д.т.н., проф., **Романов А. И.**
Научный консультант: **Пизюк Д. Л.**
Институт телекоммуникационных систем НТУУ«КПИ»
E-mail: aparadovsky@gmail.com

Быстрое развитие средств информационных технологий и тенденции усложнения космического сегмента диктуют необходимость поиска новых систем формирования цифровой телеметрической информации. Эти системы предназначены для сбора, обобщения и передачи на Землю данных о состоянии космического аппарата и его служебных систем. Установка на платформе геостационарного спутника видеокамер позволит расширить функционал существующих систем телеконтроля и даст возможность более эффективного слежения за состоянием космического аппарата.

TECHNOLOGY REALIZATION OF STRATEGIES TRANSMITTING INFORMATION IN LAN

Naidych V.R.
Scientific adviser: **Moshynska A.V.**
Institute of Telecommunication Systems NTU "KPI", Ukraine
E-mail: vikanaid@yandex.ru

In this paper investigates the modern strategy transmitting information in local networks. The actual problem is the effective use of local networks technology for the transmission of large information volumes. Basic attention is directed to technologies such as Ethernet, Wi-Fi and xDSL. Modern programmatic protocols the proposed technology and their function are investigational as to the decision of task of effective transmission to information in LAN.

ТЕХНОЛОГІЯ РЕАЛІЗАЦІЇ СТРАТЕГІЙ ПЕРЕДАЧІ ІНФОРМАЦІЇ В LAN

Найдич В.Р.
Науковий керівник: к.т.н., доц. **Мошинська А.В.**
Інститут телекомунікаційних систем НТУУ «КПІ»
E-mail: vikanaid@yandex.ru

В роботі досліджуються сучасні стратегії передачі інформації в локальних мережах. Актуальною виступає задача ефективного використання технологій локальних мереж для передачі великих об’ємів інформації. Основну увагу направлено на такі технології, як Ethernet. Wi-Fi та xDSL. Досліджуються сучасні програмні протоколи запропонованих технологій та їх функції щодо вирішення завдання ефективної передачі інформації в LAN.

APPLICATION OF GRID - SYSTEMS FOR SOLVING COMPLEX COMPUTATIONAL PROBLEMS

Omelchenko R.Yu.
Scientific adviser: Ph. D. **Romanov O.I.**
Institute of Telecommunication Systems NTUU "KPI", Ukraine
E-mail: enternadore@ukr.net

We need considerable computing power to solve large-scale problems in such areas as astrophysics, high-energy physics, nuclear fusion, geophysics and biomedicine. Grid-systems, systems that provide association disparate, geographically distributed resources into a single computing infrastructure, can be used for it. Thus, the computational elements can be both individual users' computers and computer clusters of scientific institutions. Computer network can cover the territory of individual countries and entire continents. In the work the principles of distributed computing are analyzed, in which calculation in parallel with the main work of information resources (computers, data centers, etc.) or during their downtime. SETI @ home project is considered as one of the possible ways of organization of Grid - system.

ЗАСТОСУВАННЯ ГРІД - СИСТЕМ ДЛЯ ВИРІШЕННЯ СКЛАДНИХ ОБЧИСЛЮВАЛЬНИХ ЗАДАЧ

Омельченко Р.Ю.
Науковий керівник: д.т.н, проф. **Романов О.І.**
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: enternadore@ukr.net

Для вирішення масштабних задач в таких областях, як астрофізика, фізика високих енергій, ядерний синтез, геофізика та біомедицина потрібні значні обчислювальні потужності. Для цього можуть бути використані грід – системи, що забезпечують об’єднання розрізнених, географічно розподілених ресурсів в єдину обчислювальну інфраструктуру. При цьому, обчислювальними елементами можуть бути як окремі комп’ютери користувачів, так і комп’ютерні кластери наукових установ. Обчислювальна мережа може покривати територію як окремих країн, так і цілих континентів. В роботі аналізуються принципи розподіленого комп’ютингу, в яких обчислення відбуваються паралельно з основною роботою інформаційних ресурсов (комп’ютерів, дата-центрів та ін.) чи під час їх простою. Розглянуто проект SETI @ home, як один із можливих шляхів організації грід – системи.

ADVANTAGES OF USAGE OF OPENSTACK PLATFORM FOR BUILDING INFRASTRUCTURE AS A SERVICE (IAAS)

Liashchuk A.A.
Scientific adviser: Ph.D., Associate Professor **Minochkin D.A.**
Institute of Telecommunication Systems NTU "KPI", Ukraine
E-mail: aliashchuk@outlook.com

The main trends of IT-area and the ways of implementation for “cloud” technologies are analyzed. The process of deployment and exploitation of OpenStack platform is examined. Infrastructures which are built on traditional technologies of virtualization are considered. Comparison is made and advantages of OpenStack service are marked.

ПЕРЕВАГИ ВИКОРИСТАННЯ ПЛАТФОРМИ OPENSTACK ДЛЯ ПОБУДОВИ ІНФРАСТРУКТУРИ ЯК СЕРВІСУ (IAAS)

Лящук А.А.
Науковий керівник: к.т.н, доц. **Міночкін Д.А.**
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: aliashchuk@outlook.com

Проаналізовано основні тенденції IT-ринку та напрямки впровадження «хмарних» технологій. Досліджено процес розгортання та експлуатації платформи OpenStack. Розглянуто інфраструктури, які побудовані на традиційних технологіях віртуалізації. Проведено порівняння та виділені переваги сервісу OpenStack.

AUTHENTIFICATION AND AUTHORIZATION PROCESS FOR OPENSTACK SERVICES

Kybenko A.V.
Scientific adviser: Ph.D., Associate Professor **Minochkin D.A.**
Institute of Telecommunication Systems NTU "KPI", Ukraine
E-mail: endryu-kibenko@outlook.com

Main functions of OpenStack Identity component (keystone) are analyzed. Main services which are the basis of OpenStack Identity are considered. Main concepts of Identity user management are examined.

ПРОЦЕС АУТЕНТИФІКАЦІЇ І АВТОРИЗАЦІЇ ДЛЯ ПОСЛУГ OPENSTACK

Кибенко А.В.
Науковий керівник: к.т.н., доц. **Міночкін Д.А.**
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: endryu-kibenko@outlook.com

Досліджено основні функції компоненту OpenStack Identity(keystone). Проаналізовано основні сервіси, на основі яких побудовано OpenStack Identity. Розглянуто основні концепції управління ідентифікацією користувача.

ALGORITHM OF INTERACTION OF SIP AND SS7 PROTOCOLS IN TELECOMMUNICATIONS NETWORKS ON THE BASE OF SOFTSWITCH.

Babych M.V.
Scientific adviser: **Gatturov V.K.**
Institute of Telecommunication System NTU "KPI", Ukraine
E-mail: nikolay.babych@gmail.com

Main features of interaction algorithm of ISDN networks based on OKS№7 protocol and networks based on SIP protocol with the usage of Softwitch technology. Interaction of these protocols was analyzed while providing different types of services to the consumers.

АЛГОРИТМ ВЗАЄМОДІЇ ПРОТОКОЛІВ SIP І ОКС№7 В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ НА БАЗІ SOFTSWITCH

Бабич М.В.
Науковий керівник: **Гаттуров В.К.**
Інститут телекомунікаційних систем НТУУ «КПІ», Україні
E-mail: nikolay.babych@gmail.com

Досліджено особливості алгоритму взаємодії мереж ISDN на базі протоколу ОКС№7 і мереж на базі протоколу SIP з використанням технології Softswitch. Проаналізовано взаємодію даних протоколів при надані різних послуг абонентам.

CHECKING THE PURITY OF THE ENDS OF THE FIBERS AND THEIR CLEANING

Sapa T.I.
Scientific adviser: Ph.D. **Katok V.B.**
National technical University of Ukraine «Kyiv Polytechnic Institute»
The Institute of telecommunication systems
E-mail: sapatatiana@gmail.com

The problem of contamination of the end faces of optical fibers is shown. Types of contamination of the end faces of optical fibers. The sources of such contaminants. Description of different types of cleaning the end types of optical fibers. The devices required for cleaning the end types.

ПРОВЕРКА ЧИСТОТЫ ТОРЦОВ ВОЛОКНА И ИХ ОЧИСТКА

Сапа Т.И.
Научный руководитель: к.т.н. **Каток В.Б.**
Институт телекоммуникационных систем НТУУ «КПИ»
E-mail: sapatatiana@gmail.com

Проблема загрязненности торцов волоконных световодов. Виды загрязнений торцов волоконных световодов. Источники таких загрязнений. Описание разных видов очистки торцов волоконных световодов. Устройства, необходимые для очистки торцов.

ANALYSIS OF PARAMETERS OF VOIP NETWORK, THAT AFFECT VOICE QUALITY

Dmytryev V.V.
Scientific adviser: **Maksimov V.V.**
Institute of Telecommunication Systems NTU "KPI", Ukraine
E-mail: dmytryev.seo@gmail.com

The analysis of the VoIP network parameters that affect voice quality, namely the loss of IP-packets, causes of delay in voice transmission, bandwidth.

АНАЛІЗ ПАРАМЕТРІВ VOIP МЕРЕЖІ, ЯКІ ВПЛИВАЮТЬ НА ЯКІСТЬ ПЕРЕДАЧІ ГОЛОСУ

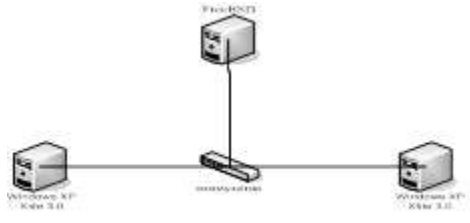
Дмитриєв В.В.
Науковий керівник: **Максимов В.В.**
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: dmitriev.seo@gmail.com

Проведено аналіз параметрів VoIP мережі, які впливають на якість передачі голосу, а саме: втрату IP-пакетів, причини затримки при передачі мови, пропускну здатність.

CONFIGURING VOIP NETWORK BASED ON ASTERISK

Buglak D. A.
Scientific adviser: Assistant Department of Telecommunication Systems
Pidgyrska T.V.
Institute of Telecommunication Systems NTU "KPI", Ukraine
E-mail: buga200894@gmail.com

To configure VoIP network based on Asterisk, we in fact want to install a virtual machine-based installation of FreeBSD (or Debian / Linux by choice), which will act as servers voice. Immediately virtual machine is using software VirtualBox, as well as the operating system we use, as described above, FreeBSD (or Debian / Linux to choose from). Also, both computers must install SIP-phone X-Lite. So, after the above transactions, we received IP network diagram is shown below.

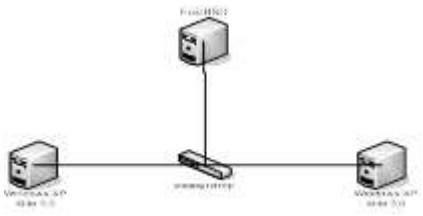


Network IP telephony

НАЛАШТУВАННЯ VOIP МЕРЕЖІ НА БАЗІ ASTERISK

Буглак Д. А.
Науковий керівник: асистент кафедри Телекомунікаційних систем **Підгурська Т.В.**
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: buga200894@gmail.com

Для того, щоб налаштувати VoIP мережу на базі Asterisk , нам по факту потрібно інсталювати віртуальну машину на базі встановлення FreeBSD (або Debian/Linux на вибір), яка буде виконувати роль сервера голосового зв'язку. Безпосередньо віртуальна машина працює за допомогою програмного забезпечення VirtualBox, а в якості операційної системи ми використовуємо, як сказано вище, FreeBSD (або Debian/Linux на вибір). Також на обидва комп'ютера потрібно встановити SIP-телефон X-Lite. Таким чином, після проведення вищеназваних операцій ми отримали IP мережу, схема якої показана нижче.



Мережа IP телефонії

RESEARCH OF THE MULTISERVICE TELECOMMUNICATION NETWORK BASED ON THE 802.11N STANDARD

Osypchuk I. S.
Scientific adviser: **Osypchuk S.A.**
Institute of Telecommunication Systems, NTU "KPI", Ukraine
E-mail: osypchuk_ivan@i.ua

Multiservice network based on two MikroTik SXT Lite5 routers was researched. These devices operate in the IEE 802.11n standard. Experimental results have shown that this network is able to perform audio streaming in MP3 format at a rate of 145 kbit /s, video streaming in TS (MPEG-2 + MPGA) format at a rate of 5.6 Mbit/s and data transfer at a rate of 69.9 Mbit/s at the same time.

ИССЛЕДОВАНИЕ МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ НА ОСНОВЕ СТАНДАРТА 802.11N

Осипчук И. С.
Научный руководитель: **Осипчук С. А.**
Институт телекоммуникационных систем, НТУУ «КПИ», Украина
E-mail: osypchuk_ivan@i.ua

Была исследована мультисервисная сеть, построенная на базе двух устройств MikroTik SXT Lite5, работающих в стандарте 802.11n. Результаты экспериментальной части показали, что она способна выполнять аудио-стриминг в формате MP3 со скоростью 145 Кбит/с, видео-стриминг в формате TS (MPEG-2 + MPGA) со скоростью 5,6 Мбит/с и передачу данных со скоростью 69,9 Мбит/с одновременно.

SOLVING PROBLEMS OF DATA MERGE IN IoT ARCHITECTURE THROUGH JOINT DIRECTOR OF LABS

Bugaenko Y.M.
Scientific adviser: **Kurdecha V.V.**
Institute of Telecommunication Systems NTU "KPI", Ukraine
E-mail: yura.buhaenko@gmail.com

The report provides an overview of the model based on Joint Director of Labs to optimize data in the Internet of Things (IoT) and addressing data fusion uniform data to reduce load on the server IoT. The problem of merging and analysis is one of the main tasks to be solved to create a full-fledged Internet of things. There are different currently used models to merge data, but the best one is the Joint Director of Labs (JDL). Joint Director of Labs model includes five levels:

- Level 0 Sensor Processing.
- Level 1 Object Identification.
- Level 2 Object Aggregation of similar entities.
- Level 3 Impact analysis and Risk militating.
- Level 4 Proccess refinement.

The model was developed to determine the synthesis process data. Each level has a certain task at each level and some information is processed and passed to the upper level for further processing and analysis. The volume of information to be processed in the system will be huge, given the dynamic addition of nodes in sensor IoT. Also the comparison of its own, alternative model data.

ВИРІШЕННЯ ПРОБЛЕМИ ЗЛИТТЯ ДАНИХ В IoT ЗА ДОПОМОГОЮ АРХІТЕКТУРИ JOINT DIRECTOR OF LABS

Бугаєнко Ю.М.
Науковий керівник: **Курдеча В.В.**
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: yura.buhaenko@gmail.com

В доповіді представлено огляд моделі Joint Director of Labs для оптимізації обробки даних в Internet of Things (IoT) та вирішення проблеми злиття даних однорідних даних для зменшення навантаження на сервер IoT. Проблема злиття і аналізу даних є одним із головних завдання, що потрібно вирішити для створення повноцінного Інтернету речей. Існують різні моделі злиття даних, що наразі використовується, але найбільш оптимальною з них є Joint Director of Labs (JDL). Joint Director of Labs модель включає в себе п'ять рівнів для методології синтезу:

- рівень 0 для попередньої обробки,
- рівень 1 для об'єкта уточнення,
- рівень 2 для уточнення ситуації,
- рівень 3 для уточнення загроз,
- рівень 4 для процесу уточнення.

Модель була розроблена для визначення процесу синтезу даних. Кожен рівень має певні задачі, і на кожному рівні певна інформація обробляється і передається на верхні рівні для подальшої обробки і аналізу. Обсяг інформації, яка буде оброблятися в системі буде величезним, враховуючи динамічне додавання вузлів датчиків в IoT. Також проведено порівняння з власною, альтернативною моделлю обробки даних.

THE MODIFIED NETWORK ARCHITECTURE INTERNET OF THINGS BY USING REPROGRAMMING MICROCONTROLLER

Pokhylinskiy S.A.
Scientific adviser: **V.V. Kurdecha**
Institute of Telecommunication Systems NTU "KPI", Ukraine
E-mail: Sergey.Pokhylinskiy@gmail.com

Today, there are many so-smart things are called, but it is more automated than the smart thing, because in all stages of the problem is still present people.

МОДИФИЦИРОВАННАЯ АРХИТЕКТУРА СЕТИ INTERNET OF THINGS ЗА СЧЕТ ИСПОЛЬЗОВАНИЯ РЕПРОГРАММИРУЕМОГО МИКРОКОНТРОЛЛЕРА

Похилинский С.А.
Научный руководитель: **Курдеча В.В.**
Институт телекоммуникационных систем НТУУ «КПИ», Украина
E-mail: Sergey.Pokhylinskiy@gmail.com

На сегодняшний день существует множество так званых умных вещей, но это скорее автоматизация, нежели умные вещи, ведь во всех этапах выполнения задачи по прежнему присутствует человек.

COMPARATIVE ANALYSIS OF TECHNOLOGY BROADBAND SERVICES BASED ON MPLS TECHNOLOGY

Bovtruk A. Y.
Scientific adviser: **Sozonnyk H.D.**
Institute of Telecommunication Systems NTU "KPI", Ukraine
E-mail: bovtrukau@gmail.com

Researched criteria that meet the requirements of private customers broadband services and telecommunications providers for the organization of virtual networks on the basis of technology MPLS. For selected criteria comparative analysis of options for building a network based on protocols BGP-MPLS VPN and VPLS.

ПОРІВНЯЛЬНИЙ АНАЛІЗ ТЕХНОЛОГІЙ НАДАННЯ ШИРОКОСМУГОВИХ ПОСЛУГ НА БАЗІ ТЕХНОЛОГІЇ MPLS

Бовтрук А. Ю.
Науковий керівник: **Созонник Г.Д.**
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: bovtrukau@gmail.com

Досліджені критерії, що відповідають вимогам приватних замовників широкосмугових послуг та провайдерів телекомунікацій щодо організації віртуальних мереж на базі технології MPLS. За обраними критеріями проведений порівняльний аналіз варіантів побудови мережі на базі протоколів BGP-MPLS VPN та VPLS.