



**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
"КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
ІМЕНІ ІГОРЯ СІКОРСЬКОГО"**

**ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ
НДІ ТЕЛЕКОМУНІКАЦІЙ**

**Чотирнадцята міжнародна
науково-технічна конференція
" ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ"
і**

**Дванадцята міжнародна науково-технічна конференція
студентів та аспірантів «ПЕРСПЕКТИВИ РОЗВИТКУ
ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ
ТЕХНОЛОГІЙ ТА СИСТЕМ»**

Присвячено Дню науки та Всесвітньому Дню телекомунікацій

13–17 квітня 2020 року

Матеріали конференції

м. Київ



**NATIONAL TECHNICAL UNIVERSITY OF UKRAINE
“IGOR SIKORSKY KYIV POLYTECHNIC INSTITUTE”**

**INSTITUTE OF TELECOMMUNICATION SYSTEMS
RESEARCH INSTITUTE OF TELECOMMUNICATIONS**

**Fourteenth International Scientific Conference
"MODERN CHALLENGES IN TELECOMMUNICATIONS"**

and

**Twelfth 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 13-17, 2020

Conference proceedings

Kyiv

XIV Міжнародна науково-технічна конференція "**Перспективи телекомунікацій**" ПТ-2020: Збірник матеріалів конференції. К.: КПІ ім. Ігоря Сікорського, 2020. – с.386.

XIV International Scientific Conference "**Modern Challenges in Telecommunications**" MCT-2020. Conference proceedings. Kyiv. Igor Sikorsky Kyiv Polytechnic Institute, 2020 – p. 386.

XII Міжнародна науково-технічна конференція студентів та аспірантів «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем» ПРІТС 2020: Збірник тез конференції. К.: КПІ ім. Ігоря Сікорського, 2020.

Збірник містить матеріали пленарних і секційних доповідей, представлених на Чотирнадцятій міжнародній науково-технічній конференції "Перспективи телекомунікацій" (ПТ 2020) та Дванадцятій міжнародній науково-технічній конференції студентів та аспірантів «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем» (ПРІТС 2020), дати проведення 13–17 квітня 2020 р. в м. Києві.

Електронна версія Збірника матеріалів Міжнародної науково-технічної конференції "Перспективи телекомунікацій" (кожна стаття має свою URL-адресу) за посиланнями:

<http://conferenc.its.kpi.ua/proc/issue/archive>,
<http://journals.urau.ua/> (ISSNonline 2664-305).

Робочими мовами конференцій є українська, російська та англійська.

У збірник включені матеріали конференції за такими секціями:

1. Достовірне передавання сигналів та інформації в телекомунікаційних системах.
2. Засоби телекомунікацій та кабельні системи і технології.
3. Технології транспортних телекомунікаційних систем та мережні технології.
4. Безпроводові телекомунікаційні системи та технології, системи 5G, Інтернет речей.
5. Інформаційні технології в телекомунікаціях.
6. Сенсорні мережі та прикладні аспекти застосування телекомунікаційних технологій.
7. Системна й програмна інженерія інфокомунікацій.
8. Семінар: Modern information and telecommunication trends (спілкування виключно на англійській мові).

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

Співголови конференції "Перспективи телекомунікацій":

ІЛЬЧЕНКО М.Ю. – науковий керівник, директор Інституту телекомунікаційних систем Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», академік НАНУ, д.т.н., професор;

БАРАНОВ О.А. – керівник Центру теоретико-правових проблем інформаційної сфери Науково-дослідного інституту інформатики і права Національної академії правових наук України, д.ю.н., професор.

Організатори конференції:

Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», ІТС, НДІТ;

Міжнародний науково-технічний журнал «Information and Telecommunication Sciences» ISSN: 2312-4121.

Спонсори конференції:

Організації та підприємства, які беруть участь в науково-інноваційній діяльності та в працевлаштуванні випускників ІТС, а також всі бажаючі.

Координатор Програмного комітету:

КРАВЧУК С.О. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ.

Члени Програмного комітету "Перспективи телекомунікацій":

БОГУШ В. М. - к.т.н., доц., НАУ, Київ;

ГЛОБА Л.С. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;

ГУДИМЕНКО І.А. - Dr.-Eng. at T-Systems MSC, Дрезден, Німеччина;

ЖУК С.Я. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;

ЗАВИСЛЯК І.В. - д.ф.м.н., проф., КНУ ім. Т. Шевченко, Київ;

КАПШТИК С.В. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;

КАТОК В.Б. - к.т.н., проф., ПАТ «Укртелеком», Київ;

КИСЕЛЬОВ Стів - PhD St. of Friedrich-Alexander-University, Нюрнберг, Німеччина;

КОЗЕЛКОВ С.В. - д.т.н., проф. ДУТ, Київ;

КОТ Т.М. - Dr.-Eng., Solutions Architect, NVision Czech Republic, Прага, Чехія;

ЛЕМЕШКО О.В. - д.т.н., проф., ХНУРЕ, Харків;

ЛИСЕНКО О.І. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
ЛУНТОВСЬКИЙ А.О. - Prof. at BA Dresden University, Дрезден, Німеччина;
МАКСИМОВ В.В. - к.т.н., доц. КПІ ім. Ігоря Сікорського, Київ;
МОШИНСЬКА А.В. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
НАЗАРЕНКО О.І. – факультет лінгвістики КПІ ім. Ігоря Сікорського, м. Київ;
НАРИТНИК Т.М. - к.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
ПОПОВ В.І. - д.м.-ф.н., проф., РТУ, м. Рига, Латвія;
ПРАВИЛО В.В. – к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
РОМАНОВ О.І. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
РОМАНЮК В.А. - д.т.н., проф. ВІТІ, Київ;
СЕРГІЄНКО М.І. – ст. викладач каф. ІЕ, ІЕЕ, КПІ ім. Ігоря Сікорського, Київ;
СКУЛИШ М.А. - д.т.н., с.н.с., КПІ ім. Ігоря Сікорського, Київ;
СТРИЖАК О.Є. - к.т.н., НЦ «Мала АНУ», Київ;
ТЕНШИ Хара - Dr.-Eng. Technical University of Dresden, Дрезден, Німеччина;
ТОЛЮПА С.В. – д.т.н., проф., НУ ім. Т.Г.Щевченка, Київ;
ТРУБІН О.О. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
УРИВСЬКИЙ Л.О. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
ФЕЛЬДМАНН Маріус - Dr.-Eng. Technical University of Dresden, Дрезден, Німеччина;
ЧЕЧЕЛЬНИЦЬКИЙ В.Я. - д.т.н., проф., ОНПУ, Одеса;
ЧУМАЧЕНКО С.М. - д.т.н., с.н.с., НУХТ, Київ;
ШЕЛКОВНИКОВ Б.М. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
ШПІЛЬНЕР Йозеф - Dr. at ZHAW School of Engineering, Цюрих, Вінтертур, Швейцарія;
ЯВІСЯ В.С. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
ЯКОРНОВ Є.А. - к.т.н., проф., КПІ ім. Ігоря Сікорського, Київ.

Технічний комітет:

1. Дуля Ю.А. – головний бухгалтер НДІ ТК, т. 236-95-04.
2. Березовська О.В. – реєстрація, забезпечення документообігу, т. 204-98-21.
3. Мікляєв О.В. – технічне обслуговування електронної техніки, т. 204-98-21.
4. Іванова Т.Л. – оформлення конференції на сайті ІТС, поселення т. 204-98-91.
5. Головай О.М. – технік I категорії.

Адреса для листування, телефони, e-mail:

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

Адреса проведення конференції:

Конференція відбулась on-line за допомогою сервісу для проведення відеоконференцій та вебінарів ZOOM.

ЗМІСТ

Секція 1. Достовірне передавання сигналів та 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:

Максимов В.В., Храповицький І.А.

ДОСЛІДЖЕННЯ КОМПОЗИТНИХ КОДІВ БАРКЕРА 18

Вакуленко О.В., Єрохін В.Ф.

ЗАГАЛЬНІ ПІДХОДИ ЩОДО ОЦІНКИ ЙМОВІРНОСТІ
ФУНКЦІОНУВАННЯ ЛІНІЙ ЗВ'ЯЗКУ В УМОВАХ ВОГНЕВОГО ТА
РАДІОЕЛЕКТРОННОГО ПРИДУШЕННЯ 21

Козак А.Ю., Могилевич Д.І.

ОГЛЯД МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ОБСЛУГОВУВАННЯ В
СУЧАСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ 25

Турчин Я.В., Кононова І.В.

АНАЛІЗ ВИКОРИСТАННЯ ПРОТОКОЛІВ IPSEC ТА SSL В
КОРПОРАТИВНИХ МЕРЕЖАХ 28

Уривський Л. О., Корнієнко А. А.

ГРАНИЧНЕ ЗНАЧЕННЯ БЛОКУ КОДІВ ХЄМІНГА ПРИ ЗАДАНИХ
ВИМОГАХ ЩОДО ДОСТОВІРНОСТІ ПРИЙОМУ 31

Новіков В.І.

АНАЛІТИЧНА МОДЕЛЬ БЕЗПРОВОДОВОГО КАНАЛУ СЕНСОРНОЇ
МЕРЕЖІ В УМОВАХ ЗАВМИРАНЬ І ВИПАДКОВОГО РОЗКИДУ
ПАРАМЕТРІВ ПРИЙМАЛЬНО-ПЕРЕДАВАЧІВ 34

Уривський Л.О., Шмігель Б.О.

ПОРІВНЯННЯ ЗАВАДОСТІЙКОСТІ ШИРОКОСМУГОВИХ ТА
ВУЗЬКОСМУГОВИХ СИГНАЛІВ ЗВ'ЯЗКУ В УМОВАХ НИЗЬКОЇ
ЕНЕРГЕТИКИ 38

Гогу О.П., Гаттуров В. К.

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ НАДАННЯ ПОСЛУГ В
ВІРТУАЛЬНОМУ СЕРЕДОВИЩІ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ
NGN НА БАЗІ IMS 41

Мошинська А.В.

ОЦІНКА ІНФОРМАЦІЙНОЇ ЕФЕКТИВНОСТІ СТРАТЕГІЙ ПЕРЕДАЧІ
ІНФОРМАЦІЇ В МУЛЬТИСЕРВІСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ
СИСТЕМАХ 44

Григоренко О.Г., Вістунів В.Д. ОРГАНІЗАЦІЯ ШИРОКОСМУГОВОГО ДОСТУПУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ PON	47
Григоренко О.Г., Кочева Н.С. ОСОБЛИВОСТІ ОПТИЧНИХ МЕРЕЖ ДЛЯ ЗАБЕЗПЕЧЕННЯ ВИМОГ ТЕХНОЛОГІЇ 5G	50
Григоренко О.Г., Полікарпова Ю.Г. РЕКОМЕНДАЦІЇ ЩОДО ПОКРАЩЕННЯ БЕЗПЕКИ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ.....	53
Волік Д. В., Григоренко О.Г. ПОБУДОВА ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ НА ОСНОВІ ОБЛАДНАННЯ ФІРМИ CISCO	56
Носков В.І. ПІДХОДИ ЩОДО РОЗРОБКИ РЕКОМЕНДАЦІЙ ПО ВИБОРУ ВИДУ ЛІНІЙНОГО СИГНАЛУ В МЕРЕЖАХ ДОСТУПУ SHDSL	59
Буханець О.С., Бердников О.М. МАКСИМАЛЬНЕ НАБЛИЖЕННЯ ШВИДКОСТЕЙ ПЕРЕДАЧІ ВОСП ХМ ДО ГРАНИЧНИХ МЕЖ	62
Ветошко І.П., Носков В.І. ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ ТЕХНОЛОГІЇ ПЕРЕДАЧІ ГОЛОСУ В МЕРЕЖІ LTE	65

Секція 2. Засоби телекомунікацій та кабельні системи і технології

Співголови:

д.т.н., проф. Трубін О.О., к.т.н., проф. Якорнов Є.А., к.т.н., доц. Шелковніков Б.М.

Доповідачі:

Trubarov I.V. DESIGN AND OPTIMIZATION OF COAXIAL-FED RECTANGULAR PATCH ANTENNA FOR 2.4 GHZ FREQUENCY BAND	68
Trubarov I.V. DESIGN OF A MICROSTRIP FILTER FOR 5 GHZ BAND USING DIFFERENT NUMERICAL METHODS.....	71
Trubarov I.V. DESIGN AND OPTIMIZATION OF COAXIAL-FED CIRCULAR PATCH ANTENNA FOR 2.4 GHZ FREQUENCY BAND	74

Ігнатченко М.М., Авдєєнко Г.Л. ПРИЗНАЧЕННЯ ТА ЗАДАЧІ СИСТЕМ МОНИТОРИНГУ ДЖЕРЕЛ РАДІО- ВИПРОМІНЮВАННЯ НА БАЗІ ВИКОРИСТАННЯ ПРИСТРОЇВ SDR.....	77
Авдєєнко Г.Л., Мар'яненко А. О. ЗАСТОСУВАННЯ ТРАНСИВЕРУ NUAND BLADERF X40 SDR ДЛЯ ФОРМУВАННЯ ТЕЛЕВІЗІЙНИХ СИГНАЛІВ СТАНДАРТУ DVB-S2	80
Накоренко А.А., Губар В.Г. ПРИСТРІЙ ПЕРЕВІРКИ ДЖГУТІВ	83
Trubin A. A. WAVEGUIDE DISTRIBUTION OF COUPLED DIELECTRIC RESONATOR MODES IN THE UNIFORM LATTICES	86
Trubin A. A. ADAPTIVE PLANAR ANTENNAS ON LATTICES OF ROTATING DIELECTRIC RESONATORS.....	89

Секція 3. Технології транспортних телекомунікаційних систем та мережні технології

Співголови:

д.т.н., проф. Романов О.І., д.т.н., проф. Лемешко О.В., д.т.н., проф. Чечельницький В.Я.

Доповідачі:

Saychenko I.O. Kamarali R.V. Romanov M.O. OPTIMIZE OPTICAL DATA NETWORKS USING SDN TECHNOLOGIES	92
Кочура М.Ю., Романов М.О. ПОБУДОВА МЕРЕЖІ SDN З ВИКОРИСТАННЯ ПЛАТФОРМИ SEBA	95
Підпалій О.І., Романов О.І. АНАЛІЗ ВРАЗЛИВОСТІ БЕЗДРОТОВОЇ МЕРЕЖІ WI-FI З НОВИМ ПРОТОКОЛОМ ЗАХИЩЕНОСТІ WPA3	98
Маньківський В.Б., Педько А.Д. МЕТОД ЗМЕНШЕННЯ ЧАСУ ДОСТАВКИ ПОВІДОМЛЕНЬ В IP МЕРЕЖІ ЗА РАХУНОК МОДИФІКАЦІЇ ПРОТОКОЛУ UDP	102
Маньківський В.Б., Педько А.Д. КОНЦЕПЦІЯ ГРАНИЧНИХ ОБИЧИСЛИНЬ В МЕРЕЖІ МОБІЛЬНОГО ОПЕРАТОРА.....	105
Романов О.І., Шихов М.С. ПОБУДОВА КОНТРОЛЕРА МЕРЕЖІ SDN З ВИКОРИСТАННЯ ХМАРНИХ РЕСУРСІВ.....	109

Піталова М.Д., Мікляєв Г.О. БАГАТОВУЗЛОВА МЕРЕЖА SDN З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ LI-FI	112
Полуденний О. М., Романов О. І. ВИКОРИСТАННЯ ПРЕДМЕТНО-ОРІЄНТОВАНОЇ МОВИ ПРОГРАМУВАННЯ P4 ДЛЯ ПОБУДОВИ IMS	116
Літвінов Є.А., Романов О.І. МОДЕЛЬ ДОСЛІДЖЕННЯ СИГНАЛІВ ОПТИЧНОГО ТРАКТУ З ВИКОРИСТАННЯМ SDR ТРАНСІВЕРА ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ GNURADIO	119
Данильченко В.О., Кононова І.В. АНАЛІЗ ВАРІАНТІВ ПЕРЕХОДУ ДО МЕРЕЖ НАСТУПНОГО ПОКОЛІННЯ З ВИКОРИСТАННЯ ТЕХНОЛОГІЇ NG-PON2	122
Литовченко К.А., Романов О.І. АНАЛІЗ ПРИНЦИПІВ ПОБУДОВИ MPLS L3 VPN.....	125
Бондар О.Р., Верес Л.А. РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В МЕРЕЖІ ПІДПРИЄМСТВА НА ОСНОВІ МЕТОДІВ ЯКОСТІ ОБСЛУГОВУВАННЯ.....	128
Романов О.І., Верес Л.А. Нестеренко М.М. МЕТОДИКА РОЗРАХУНКУ БЕЗВІДМОВНОЇ РОБОТИ СИСТЕМИ IMS НА БАЗІ ВІРТУАЛЬНИХ МАШИН	132
Нестеренко М.М., Коломійчук О.А., Фесьоха Н.О. АРХІТЕКТУРА МЕРЕЖІ ІР-ТЕЛЕФОНІЇ НА ОСНОВІ SOFTSWITCH...	135
Тріска Н.Р. ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ ASON В СУЧАСНИХ ТРАНСПОРТНИХ МЕРЕЖАХ.....	139
Тріска Н.Р. ВИКОРИСТАННЯ ПРОГРАМНОГО ПАКЕТУ SYNC ARCHITECT ДЛЯ ПРОЕКТУВАННЯ МЕРЕЖ СИНХРОНІЗАЦІЇ	142
Бирюков Н.Л., Тріска Н.Р. ИСПОЛЬЗОВАНИЕ ПУАССОНОВСКОЙ МОДЕЛИ ДЛЯ АНАЛИЗА ПРОСКАЛЬЗЫВАНИЯ В ПЛЕЗИОХРОННОМ СОЕДИНЕНИИ	145
Атаманчук М.В, Романов А.О. КОНВЕЄРНА ОБРОБКА ДАНИХ В КОМУТАТОРАХ МЕРЕЖІ SDN	148
Романов О.І., Нестеренко М.М., Фесьоха Н.О. ЗАХИЩЕНІСТЬ ІНФОРМАЦІЙНИХ СИСТЕМ ПРИ ВИКОРИСТАННІ ТЕХНОЛОГІЙ ВІРТУАЛІЗАЦІЇ	151

**Секція 4. Безпроводові телекомунікаційні системи
та технології, системи 5G, Інтернет речей**

Співголови: д.т.н., проф. Кравчук С.О., к.т.н., доц. Капштик С.В.

Доповідачі:

Кравчук І.М.

РЕГУЛЮВАННЯ ВИКОРИСТАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ
АПАРАТІВ ДЛЯ МОНІТОРИНГУ ОБ'ЄКТІВ.....155

Афанасьєва Л.О.

АЛГОРИТМ ВИБОРУ ДОПОМІЖНИХ ВУЗЛІВ ДЛЯ
БЕЗПРОВОДОВОЇ КООПЕРАТИВНОЇ РЕТРАНСЛЯЦІЇ З
ПЕРЕХОПЛЮВАЧЕМ 158

Кравчук С.О.

MOBILE INFOCOMMUNICATION SYSTEMS.....161

Хлівний Д.Ю., Кравчук С.О.

АЛГОРИТМ РОЗМІЩЕННЯ БАЗОВИХ СТАНЦІЙ ДЛЯ
МАСШТАБНИХ ГЕТЕРОГЕННИХ МЕРЕЖ LTE 165

Афанасьєва Л.О., Кравчук С.О., Шевченко І.І., Чуб М.М.

БЕЗПРОВОДОВА КООПЕРАТИВНА РЕТРАНСЛЯЦІЯ З
ТЕХНОЛОГІЄЮ HARQ 168

Рисцова К.І., Остапов О.А., Кравчук С.О.

УЗАГАЛЬНЕНА СТРУКТУРА СИСТЕМИ МОБІЛЬНИХ
ІНФОКОМУНІКАЦІЙ.....171

Кравчук С.О., Кайденко М.М., Афанасьєва Л.О., Кравчук І.М.

ЕКСПЕРИМЕНТАЛЬНЕ ВІДПРАЦЮВАННЯ РЕТРАНСЛЯЦІЙНИХ
ВУЗЛІВ СУЗІР'Я ДРОНІВ.....175

Правило В.В., Кормульов О.С.

МЕТОДИ ЗАБЕЗПЕЧЕННЯ ЗАДАНИХ ПОКАЗНИКІВ БЕЗПЕКИ В
5G МЕРЕЖАХ.....178

Федоров С.О., Правило В.В.

НАДШИРОКОСМУГОВИЙ МОБІЛЬНИЙ ЗВ'ЯЗОК ЯК ОДИН ІЗ
ПЕРШИХ СЕРВІСІВ 5G.....181

Авдєєнко Г.Л., Якорнов Є. А.

МЕТОД ПРОСТОРОВОГО ФОКУСУВАННЯ ЯК СПОСІБ
ФОРМУВАННЯ ЕЛЕКТРОМАГНІТНИХ ХВИЛЬ ЗІ СФЕРИЧНИМИ
ФАЗОВИМИ ФРОНТАМИ ДЛЯ ПІДВИЩЕННЯ ПРОДУКТИВНОСТІ
РАДІОРЕЛЕЙНИХ ЛІНІЙ 184

Денисенко Н. І., Авдєєнко Г. Л.

ОЦІНКА ЕНЕРГЕТИЧНОГО ПОТЕНЦІАЛУ ДЛЯ ЛІНІЙ
РАДІОЗВ'ЯЗКУ «ТОЧКА-ТОЧКА» НА БАЗІ ТРАНСІВЕРІВ DWM
1000 187

Свіржевська А.І. ПРОБЛЕМИ ПРОЕКТУВАННЯ ПРИЛАДІВ ДЛЯ МЕРЕЖ 5G МІЛІМЕТРОВОГО ДІАПАЗОНУ	190
Піхота К.В., Кононова І.В. АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ ПРИСТРОЇВ ТА ПОСЛУГ ІНТЕРНЕТУ РЕЧЕЙ	193
Губар В.Г., Якименко О.О. ІНКУБАТОР ДЛЯ ЯЄЦЬ З ТЕХНОЛОГІЄЮ INTERNET OF THING	196
Сергієнко А.В., Губар В.Г. ДИСТАНЦІЙНО-ПРОГРАМОВАНИЙ КОНТРОЛЕР ДАТЧИКІВ ТА ПРИСТРОЇВ	199
Kremenetskaya Y.A., Makarenko A.O., Hetmanets O.V., Trintina N.A. FUTURE 6G NETWORK FUNCTIONALITY AND PERFORMANCE	202

Секція 5. Інформаційні технології в телекомунікаціях

Співголови:

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

Доповідачі:

Корман Н.А., Могилевич Д.І. АНАЛІЗ ТЕХНОЛОГІЙ ПОБУДОВИ ВІРТУАЛЬНИХ ЗАХИЩЕНИХ МЕРЕЖ VPN	205
Глоба Л.С., Задосенко Б.О. ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ДІЯЛЬНОСТІ НАУКОВИХ УСТАНОВ МЕТОДОМ ОБРОБКИ РІЗНОРІДНОЇ СЛАБОСТРУКТУРОВАНОЇ ІНФОРМАЦІЇ.....	209
Безвугляк М. С., Курдеча В. В. ЗАХИСТ ІНФОРМАЦІЇ В МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ НА ОСНОВІ REST API.....	213
Пилипчук А.А. МОДЕЛІ ІДЕНТИФІКАЦІЇ ТА АУТЕНТИФІКАЦІЇ В СИСТЕМАХ ХМАРНИХ ОБЧИСЛЕНЬ ДЛЯ ВЕБ-СЕРВЕРІВ ТА МОБІЛЬНИХ ДОДАТКІВ З ІНТЕЛЕКТУАЛЬНОЮ ПІДТРИМКОЮ ВИБОРУ	216
Пороло Є.О., Курдеча В.В. УДОСКОНАЛЕНА АРХІТЕКТУРА МЕРЕЖІ ДЛЯ ХМАРНОГО ІНТЕРНЕТУ РЕЧЕЙ.....	219

Попенко Д.В., Курдеча В.В. АНАЛІЗ МЕТОДІВ СЕРІАЛІЗАЦІЇ ОБ'ЄКТІВ ДЛЯ ПОБУДОВИ ПЛАТФОРМИ ВЕЛИКИХ ІНДУСТРІАЛЬНИХ ДАНИХ	222
Давидюк А.М., Курдеча В.В. МОДИФІКОВАНИЙ МЕТОД УПРАВЛІННЯ ІНФРАСТРУКТУРОЮ МЕРЕЖІ ПРОМИСЛОВОГО ІНТЕРНЕТУ РЕЧЕЙ	225
Ляшенко А.В. ПІДХІД ДЛЯ ПОБУДОВИ НЕЧІТКИХ ЛОГІЧНИХ ПРАВИЛ ДЛЯ ВЕЛИКИХ ДАНИХ.....	228
Савчук З.Р., Бугаєнко Ю.М. ЗАСТОСУВАННЯ НЕЧІТКИХ ЛОГІЧНИХ ПРАВИЛ ДЛЯ АНАЛІЗУ ТА СТРУКТУРИЗАЦІЇ ВЕЛИКИХ ДАНИХ	231
Остапенко М.С., Штогріна О.С. СИСТЕМА КОМП'ЮТЕРНОГО ЗОРУ ДЛЯ НАВІГАЦІЇ В ПРИМІЩЕННІ ЛЮДЕЙ З ВАДАМИ ЗОРУ	234
Куш В.С., Штогріна О.С. МЕТОД ВИЯВЛЕННЯ ВПЛИВІВ НА ПСИХОФІЗІОЛОГІЧНИЙ СТАН ЗИМІВНИКА	237
Могильний С.Б., Мініч М. А. ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ МЕТОДІВ МОНІТОРИНГУ РУХОМИХ ОБ'ЄКТІВ В СИСТЕМАХ РОЗУМНОГО БУДИНКУ	240
Глоба Л.С., Попова М.А., Юшко Н. А. АНАЛІЗ ОЦІНКИ ЯКОСТІ НАДАННЯ ПОСЛУГ ТЕЛЕКОМУНІКАЦІЙНИМ ПРОВАЙДЕРОМ	243
Адаменко І.О., Губар В.Г. ФОТОМЕТРИЧНА СИСТЕМА ВИМІРЮВАННЯ ПАРАМЕТРІВ ГАЗІВ ТА РІДИН	246
Зайченко Ю.П., Васильєв В.И., Вишталь Д.М., Любашенко Н.Д. СТРУКТУРНО-ФАЗОВОЕ УКРУПНЕНИЕ СОСТОЯНИЙ КОММУНИКАЦИОННЫХ СЕТЕЙ В ЗАДАЧАХ ОЦЕНКИ ХАРАКТЕРИСТИК ДОСТУПНОСТИ СЕТЕВОЙ УСЛУГИ	249
Подліпаєв В.О., Чепков Р.І. КОМПОНЕНТНА КОНФІГУРАЦІЯ КОГНІТВНИХ СЕРВІСІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ ПРИЙНЯТТЯ РІШЕННЯ.....	252
Гуменюк І.В., Сметанін К.В., Некрилов О.В. ЗАХИСТ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ШЛЯХОМ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ	257

**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., д.т.н., проф. Жук С.Я.

Доповідачі:

Якорнов Є.А., Цуканов О.Ф.

АЛГОРИТМ ВИЗНАЧЕННЯ ПАРАМЕТРІВ РУХУ
КВАДРОКОПТЕРІВ У МЕРЕЖАХ FANET 260

Лисенко О. І., Валуйський С.В.

УПРАВЛІННЯ МЕРЕЖЕЮ БПЛА ІЗ ВИКОРИСТАННЯМ SDN 263

Plchenko M., Zhivkov A., Akopian P., Galickiy I., Sobko T.

ATTENUATION POLES IN BAND-PASS FILTERS WITH EVEN END
ODD MODES 266

A. Zhivkov, R. Kamarali, M. Kopaniev, O. Krylach, I. Saychenko

ANOMALOUS DISPERSION AND GROUP DELAY OF
METAMATERIAL CELLS 269

Валуйський С.В., Єфименко О.С.

МЕТОД ВИЯВЛЕННЯ DOS АТАК В SDN МЕРЕЖАХ ІЗ
ВИКОРИСТАННЯМ ЕНТРОПІЇ ШЕННОНА..... 272

Нидченко И. А., Лысенко А. И.

ИНФОРМАЦИОННО-ТЕЛЕКОМУНИКАЦИОННАЯ СИСТЕМА
УПРАВЛЕНИЯ МИНИ-ТЕПЛИЦЕЙ С ИСПОЛЬЗОВАНИЕМ
СЕРВИСНОГО РОБОТА..... 275

Явіся В.С.

АНАЛІЗ СТАНУ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ LTE ПРИ
ОРГАНІЗАЦІЇ ВИСОКОШВИДКІСНОГО АБОНЕНТСЬКОГО
ДОСТУПУ 278

Явіся В.С., Лисенко О.І.

СПОСІБ ПІДВИЩЕННЯ ЯКОСТІ КАНАЛУ УПРАВЛІННЯ
ДРОНАМИ..... 281

Явіся В.С., Явіся Д.В.

АНАЛІЗ СПОСОБІВ ОТРИМАННЯ ДАНИХ ДЛЯ СИСТЕМ
КЕРУВАННЯ ПОЛОЖЕННЯМ НАНОСУПУТНИКА..... 285

Осинський А.К., Петрова В.М.

БАЛАНСИРОВКА ЭНЕРГЕТИЧЕСКИХ ХАРАКТЕРИСТИК
СЕНСОРОВ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ 289

Якорнов Е.А., Цуканов О.Ф.

ВИЗНАЧЕННЯ ВЗАЄМНОГО РОЗТАШУВАННЯ УГРУПОВАННЯ
КВАДРОКОПТЕРІВ ПІД ЧАС МОНІТОРИНГУ НАЗЕМНОЇ
ОБСТАНОВКИ В НАДЗВИЧАЙНИХ СИТУАЦІЯХ 292

Штойко А.А., Петрова В.Н. РАЗВИТИЕ АЛГОРИТМОВ МАРШРУТИЗАЦИИ В МОБИЛЬНЫХ СЕНСОРНЫХ СЕТЯХ.....	295
Ковбаса А.О., Лисенко О.І. ОГЛЯД КОНЦЕПЦІЇ ПОТОКОВОЇ ОБРОБКИ ДАНИХ	298
Новіков В.І., Спаравало М.К., Лисенко О.І., Алексеева І.В. РОЗВИТОК ЕНЕРГОЗБЕРІГАЮЧОГО МЕТОДУ МОНІТОРИНГУ ЦІЛЕЙ У ЗОНАХ СПОСТЕРЕЖЕННЯ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ	301
Бондарець Я.Б., Лисенко О.І. РОЗВИТОК МЕТОДІВ ЕНЕРГОЗБЕРЕЖЕННЯ В МОБІЛЬНИХ СЕНСОРНИХ МЕРЕЖАХ	304
Товкач И.О., Жук С.Я. ФИЛЬТРАЦИЯ ПАРАМЕТРОВ ДВИЖЕНИЯ ИСТОЧНИКА РАДИОИЗЛУЧЕНИЯ НА ОСНОВЕ УГЛОМЕРНЫХ ИЗМЕРЕНИЙ СЕНСОРНОЙ СЕТИ	307
Романюк В.А., Лисенко А.И., Романюк А.В., Жук А.В. СПОСОБЫ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ СБОРА ДАННЫХ МОНИТОРИНГА С ИСПОЛЬЗОВАНИЕМ БПЛА ПРИ КЛАСТЕРИЗАЦИИ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ.....	310

Секція 7. Системна й програмна інженерія інфокомунікацій

Співголови: к.т.н., доц. Міночкін Д.А., к.т.н., доц. Явіся В.С.

Доповідачі:

Міночкін Д.А., Рибак О.О. ДОСЛІДЖЕННЯ ЗАВАДОСТІЙКОСТІ ТЕХНОЛОГІЇ LORAWAN	315
Міночкін Д.А., Юдін М.М., Малецький Л.В. АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ НА ОСНОВІ ТЕХНОЛОГІЇ БЛОКЧЕЙН В СФЕРІ ТЕЛЕКОМУНІКАЦІЙ.....	318
Міночкін Д.А., Бурлака Г.Ю., Гончаренко О.М МЕТОДИ ВИКОРИСТАННЯ BLOKCHAIN ТЕХНОЛОГІЙ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ.....	321
Поддубна М.О. ПОЄДНАННЯ ТЕХНОЛОГІЙ БЛОКЧЕЙН ТА ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПОКРАЩЕННЯ ПРОЗОРОСТІ ТА ПРИВАТНОСТІ ДАНИХ.....	324
Гребенніков В.О. ПРО ДОЦІЛЬНІСТЬ РОЗШИРЕННЯ ПОНЯТТЯ ІНФОРМАТИЗАЦІЇ	326

SEMINAR Modern information and telecommunication trends

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

Доповідачі:

Mikhnenko Yaroslav

INTERNET OF THINGS AND 5G 331

Kopaniev M., Zhivkov O., Rybak O.

“SMART STREET” MANAGEMENT SYSTEM PROTOTYPE BASED
ON THE LORAWAN PROTOCOL 334

Minochkin D., Sushyn I.

SECURE IOT DEVICE AUTHENTICATION 337

Noskova D., Minochkin D.

THE ARCHITECTURAL CONCEPT BONWIN "SMART ROOM" 340

Iatsyshin O., Maltsev A., Dykyy A., Osypchuk S.

RESEARCH AND IMPLEMENTATION OF IOT TEMPERATURE
AUTOMATED METERING PROJECT BASED ON
TELECOMMUNICATION SYSTEMS INSTITUTE 343

Shevchuk A.O., Romanov O.I.

TEMPERATURE MONITORING SYSTEM IN IOT NETWORK BASED
ON ESP8266 MICROCONTROLLER AND THINGSPEAK SERVICE 346

Uryvsky L.O., Solianikova V.Y.

METHOD OF MULTIPATH EFFECT ELIMINATION IN MOBILE
COMMUNICATIONS 349

Martynova K.G.

SCOPES TO SOLVE THE TASK OF TELECOMMUNICATION
RESOURCES DISTRIBUTION TO PROVIDE THE REQUIRED QoS 352

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

Співголови:

- ІЛЬЧЕНКО М.Ю.** – науковий керівник, директор Інституту телекомунікаційних систем Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», академік НАНУ, д.т.н., професор;
- ЯКОРНОВ Є.А.** – к.т.н., професор інституту телекомунікаційних систем КПІ ім. Ігоря Сікорського;
- ГАНЖА Я.В.** – голова студентської Ради інституту телекомунікаційних систем КПІ ім. Ігоря Сікорського.

Доповідачі:

- Москалюк С.О., кер. Якорнов Є.А.**
**АВТОКОМПЕНСАТОР ЗАВАД ДЛЯ ПРИЙМАЧІВ
РАДІОРЕЛЕЙНОГО ЗВ'ЯЗКУ.....357**
- Нидченко И. А. рук. Лысенко А. И.**
**РОЛЬ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ
ТЕХНОЛОГИЙ В ПРОЦЕССЕ ВЫРАЩИВАНИЯ ПРОДУКТОВ
ПИТАНИЯ 358**
- Нсер А.М. консульт. Рибак О.О.**
АНАЛІЗ ПРОТОКОЛУ DATA DISTRIBUTION SERVICE (DDS) 359
- Корман Н.А. кер. Могилевич Д.І.**
АНАЛІЗ РОЗВИТКУ ТЕХНОЛОГІЇ 5-ГО ПОКОЛІННЯ В УКРАЇНІ 360
- Турчин Я.В. кер. Кононова І.В.**
АНАЛІЗ ОСНОВНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ.....361
- Безвугляк М.С. кер. Курдеча В.В.**
ОСОБЛИВОСТІ ТЕХНОЛОГІЇ REST API В ІоТ 362
- Піхота К. В., кер. Кононова І.В.**
АНАЛІЗ ЗАГРОЗ ОСНОВНИХ КОМПОНЕНТІВ ІОТ 363
- Волчан Д.В., кер. Курдеча В.В.**
СИСТЕМА УПРАВЛІННЯ МЕРЕЖЕЮ MICROGRID.....364
- Карлін П.Ю., кер. Курдеча В.В.**
ПЕРСПЕКТИВИ РОЗВИТКУ ІНТЕРНЕТУ РЕЧЕЙ.....365
- Ловейкін Д.Ю. кер. Носков В.І.**
**МЕХАНІЗМ ПЕРЕНЕСЕННЯ АКТИВНОГО З'ЄДНАННЯ МІЖ
КАНАЛАМИ ЗВ'ЯЗКУ МОБІЛЬНОЇ МЕРЕЖІ.....366**
- Мартінова К.Г. кер. Уривський Л.О.**
**КОМПЛЕКСНА АНАЛІТИЧНА МОДЕЛЬ ОБСЛУГОВУВАННЯ НА
ХМАРНОМУ СЕРВЕРІ ПОВІДОМЛЕНЬ ІЗ ОЗНАКАМИ
ПРИОРІТЕТІВ.....367**

Пороло Є.О., кер. Курдеча В.В. ЗАСТОСУВАННЯ КОНЦЕПЦІЇ DATA BANK В МЕРЕЖІ ХМАРНОГО IoT	368
Попенко Д.В., кер. Курдеча В.В. ЗАСТОСУВАННЯ PROTOBUF В ІНДУСТРІАЛЬНОМУ ІНТЕРНЕТІ РЕЧЕЙ	369
Копа Р.В., кер. Штогріна О. С. ПІДХІД ДО ДОСЛІДЖЕННЯ ПСИХОФІЗІОЛОГІЧНОГО СТАНУ ЛЮДИНИ НА ОСНОВІ КОЛЬОРОВОЇ ПРЕФЕРЕНЦІЇ ТА СУБ'ЄКТИВНИХ ВІДЧУТТІВ	370
Степанов Г. О., кер. Курдеча В.В. МЕТОД ЗБОРУ ТА ОБРОБКИ ІНФОРМАЦІЇ В МЕРЕЖІ MICROGRID	371
Берлоус В.О., кер. Курдеча В.В. ПЕРСПЕКТИВА ВИКОРИСТАННЯ ІНТЕРНЕТ РЕЧЕЙ В КОНЦЕПЦІЇ “ЯКРАЗ ВЧАСНО”	372
Петров О.С., кер. Курдеча В.В. ІНФОРМАЦІЙНА БЕЗПЕКА INTERNET OF THINGS	373
Вітковський В.І., кер. Гаттуров В. К. ДОСЛІДЖЕННЯ ВПЛИВУ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ НА НАДІЙНІСТЬ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ	374
Мещерінов М.В., кер. Гаттуров В. К. ДОСЛІДЖЕННЯ СЦЕНАРІЇВ ВЗАЄМОДІЇ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ЗКС-7 З МЕРЕЖАМИ НАСТУПНОГО ПОКОЛІННЯ НА БАЗІ IMS.....	375
Скрябін С.А. кер. Носков В.І. МЕТОДИ ЗМЕНШЕННЯ РІВНЯ ІНТЕРФЕРЕНЦІЇ ВІД ЗАСТОСУВАННЯ РАДІО ПОВТОРЮВАЧІВ В МЕРЕЖАХ UMTS	376
Пявчик М.О., кер. Григоренко О.Г. РОЗГОРТАННЯ SDN В КОРПОРАТИВНИХ МЕРЕЖАХ НА БАЗІ КОНТРОЛЕРА APIC-ЕМ ФІРМИ CISCO	377
Ветошко І.П. кер. Носков В.І. ТЕХНОЛОГІЯ ПЕРЕДАЧІ ГОЛОСУ В МЕРЕЖІ LTE	378
Тушич А.М. кер. Сторчак К.П. МАШИННЕ НАВЧАННЯ З ВИКОРИСТАННЯМ TENSORFLOW	379
Мрига С.В. кер. Коваль Д.В. МАКЕТ АВТОМАТИЗОВАНОГО АНТЕННОГО ТРЕКЕРА ДЛЯ ПРИЙОМУ СИГНАЛІВ З МЕТЕОРОГІЧНИХ СУПУТНИКІВ.....	380
М’Тумбе Абї Трезор, кер. Єременко О.С. LOCALIZATION IN VEHICLE NETWORKS USING RADIO FREQUENCY IDENTIFICATION TECHNOLOGY	381
Егбе Годсон Агбара, кер. Єременко О.С. SECURITY FRAMEWORK FOR IOT DEVICES	382

Секція 1. Достовірне передавання сигналів та інформації в телекомунікаційних системах

УДК 621.382

ДОСЛІДЖЕННЯ КОМПОЗИТНИХ КОДІВ БАРКЕРА

Максимов В.В., Храповицький І.А.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: maksimov46@ukr.net, hrapovitskiy.igor@gmail.com

Research of composite Barker codes

In this paper, we consider the properties of Barker codes and on their basis we propose a method for generating composite Barker codes.

Широкопосмугові сигнали (ШПС) знаходять застосування в сучасних багатоканальних системах зв'язку з кодовим поділом каналів (CDMA, WCDMA). Такі сигнали займають смугу частот ширшу, ніж смуга частот, в якій передаються інформаційні сигнали. Основною характеристикою ШПС є база сигналу, обумовлена як добуток ширини його спектра F на його тривалість T :

$$B = F \cdot T \gg 1 \quad (1)$$

Найпростішим методом прийому ШПС є кореляційний. Найкращими кореляційними характеристиками володіють, відкриті в 1953 році, дискретні послідовності Баркера [2]. Величина максимального бічного викиду їх АКФ не перевищує $1/N$, де N - довжина кодової послідовності. Відомих послідовностей Баркера всього 8, максимальна довжина послідовності досягає 13 розрядів.

Автокореляційна функція послідовностей Баркера [3,4] має властивості скалярного добутку і автокореляційної функції і, тому, таку ж АКФ матимуть як інверсні, так і дзеркальні послідовності Баркера:

$$R(k) = \frac{1}{m} \sum_{i=0}^m c(i)c(i+k) = \frac{1}{m} \sum_{i=0}^m c_{\text{інв}}(i)c_{\text{інв}}(i+k) = \frac{1}{m} \sum_{i=0}^m c_{\text{зерк}}(i)c_{\text{зерк}}(i+k), \quad (2)$$

де $c(i)$ – канонічна послідовність Баркера, що визначається як $c(i) = c_1(i) c_2(i) \dots c_n(i)$, а $c_n(i)$ приймають значення ± 1 ; $c_{\text{інв}}(i) = (-1) c(i)$; $c_{\text{зерк}}(i) = c_n(i) c_{n-1}(i) \dots c_1(i)$.

З урахуванням (2) можна доповнити канонічні послідовності [3,4] інверсними і дзеркальними послідовностями Баркера (табл.1).

В [5] запропоновано метод формування композитних кодів Баркера, що володіють кореляційними властивостями, подібними до тих, якими володіє код Баркера, а саме: код формується шляхом перемноження двох канонічних послідовностей Баркера. Одна з них (коротка), називається утворюючою, а друга, більш довга - елементарною. В результаті перемноження короткої послідовності на довшу, виходять послідовності понад 13 розрядів. Основний викид АКФ у них дорівнює числу розрядів послідовності N , а максимальний бічний викид в позитивну область має значення близькі до 1. В [6] шляхом формування складових кодових послідовностей аналогічно способу, запропонованого в [5], отримані 12 послідовностей з довжиною N , що дорівнює 14, 21, 22, 33, 49, 77, 121, і перевищенням головного піку АКФ над позитивними бічними, рівним N . В [7] досліджена завадостійкість зворотних композитних кодів Баркера, отриманих перемноженням довгої послідовності на коротку і вказано на можливість використання їх в якості синхронізуючих слів в мережах WCDMA. В [8] описані ті ж самі складові кодові послідовності, що і в [6], але під новою назвою «сигнали Баркера-Волинської», і зазначено на можливість їх застосування, як для передачі команд, так і для синхронізації.

Таблиця №1. Послідовності Баркера.

дзеркальна	інверсна дзеркальна

[illegible]

N	Композитна послідовність Баркера 14a (2x7)

[illegible]

Таблица №2 (продовження)..

[illegible]

Наведене вище доводить, що використовуючи властивості канонічних послідовностей Баркера, можна збільшити кількість композитних послідовностей, отриманих в [6] з 12 до 48.

Література

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. — Пер. с англ. — М.: Издательский дом «Вильямс», 2003. — 1104 с.
2. Barker, R. H. "Group Synchronizing of Binary Digital Sequences". *Communication Theory*. London: Butterworth. pp. 273–287.
3. Варакин Л. Е. Системы связи с шумоподобными сигналами. — М.: Радио и связь, 1985. — 384с.
4. Баскаков С.И. Радиотехнические цепи и сигналы: Учебник. – М. Высш. школа, 1983. – 536с.
5. Банкет В.Л., Токарь М.С. «Композитные коды Баркера» // Цифрові технології №2, 2007р. С.8-17.
6. Волынская А.В. Результаты математического моделирования процесса поиска кодовых последовательностей с заданными корреляционными свойствами // Вестник УрГУПС: Науч.-техн. журнал. – Екатеринбург: УрГУПС, 2009. – № 3–4. – С. 64–71.
7. Максимов В.В., Чуприна Р.С. Обратные композитные коды Баркера // Наукові записки УНДІЗ, №1(21), 2012 г. – С.71-76.
8. Волынская А.В., Калинин П.М. Новые помехоустойчивые сигналы для интеллектуального канала телемеханики // *Fundamental Research* №11, 2012. – С.922-926.

ЗАГАЛЬНІ ПІДХОДИ ЩОДО ОЦІНКИ ЙМОВІРНОСТІ ФУНКЦІОНУВАННЯ ЛІНІЙ ЗВ'ЯЗКУ В УМОВАХ ВОГНЕВОГО ТА РАДІОЕЛЕКТРОННОГО ПРИДУШЕННЯ

¹Вакуленко О.В., ²Єрохін В.Ф.

¹*Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського*

²*Інституту спеціального зв'язку та захисту інформації КПІ ім. Ігоря
Сікорського*

E-mail: av31@bigmir.net

General approaches are in relation to estimation of probability of functioning of radio channels in the conditions of weapon and radio electronic suppression

General approaches open up in relation to estimation of probability of functioning of radio channels in the conditions of weapon and radio electronic suppression.

Для управління військами необхідно мати надійну систему зв'язку. Одним з елементів системи зв'язку є лінії зв'язку, які функціонують, під час бойових дій, в умовах вогневого та радіоелектронного придушення. Для прийняття управлінських рішень необхідно мати вихідні дані, в кількісних показниках, щодо надійності функціонування системи зв'язку так і окремих її елементів, наприклад лінії зв'язку. Тому розробка загальних підходів до оцінки ймовірності функціонування ліній зв'язку в умовах вогневого та радіоелектронного придушення під час бойових дій, являється актуальною в наш час.

Новизна. Визначена в комплексному підході до оцінки ймовірності функціонування ліній зв'язку в умовах вогневого та радіоелектронного придушення під час бойових дій.

Практична цінність. Результати дослідження доцільно використовувати при розробці національних стандартів, які визначають показники ефективності функціонування ліній зв'язку в умовах вогневого та радіоелектронного придушення під час бойових дій.

Мета дослідження. Розробити загальні підходи щодо оцінки ймовірності функціонування ліній зв'язку в умовах вогневого та радіоелектронного придушення під час бойових дій.

Об'єкт дослідження. Процес функціонування ліній зв'язку в умовах вогневого та радіоелектронного придушення під час бойових дій.

Предмет дослідження. Загальні підходи щодо оцінки ймовірності функціонування ліній зв'язку в умовах вогневого та радіоелектронного придушення під час бойових дій.

Незалежно від показників функціонування, які визначені для ліній зв'язку діючими Державними стандартами, користувача у кінцевому випадку цікавить – працює лінія зв'язку або ні. Якщо акцентувати увагу на більш «тонких» характеристиках, наприклад, статистика тривалості переривань у зв'язку та тривалості безперервної справної роботи, то в повній мірі визначається оцінка якості функціонування лінії зв'язку по величині середньої ймовірності її справного функціонування. Така оцінка може здатися грубою, однак при орієнтації конструйованого тут показника якості функціонування ліній зв'язку, а також при врахуванні статистики переривань зв'язку та неперервної справної роботи виявляється вкрай громіздким і як правило не застосовується на практиці. Це призводить до

необхідності вивести допустимий час переривання у зв'язку в розряд обмежень. У загальному випадку працездатність лінії зв'язку залежить від: технічної (експлуатаційно-технічної) надійності; надійності зв'язку, обумовленої характером поширення радіохвиль (тобто надійності по завмираннях) або дрейфом коефіцієнта ослаблення в кабельних лініях зв'язку; радіоелектронного придушення (РЕП) противником; вогневого впливу противника.

Природньо вважати показники технічної надійності незалежними від вогневого, радіоелектронного придушення і від надійності зв'язку за завмираннями. Однак, імовірність прийняття рішення противником на вогневе придушення (ВП) в загальному випадку може залежати від ймовірності прийняття рішення на РЕП [1, 3]. Дійсно, ймовірність прийняття рішення на РЕП прийнято визначати у загальному випадку як:

$$P_{rp} = \prod_{i=1}^n P_i, \quad i=1, 2, \dots, n.$$

Тут P_i – окремі ймовірності, що визначаються з подій, які можуть мати місце під час прийняття рішення на РЕП. Мають місце наступні залежності:

$$P_{rp} = P_{ip} P_{dp} P_{in}, \quad (1)$$

де P_{ip} – ймовірність розкриття лінії зв'язку із заданою повнотою;

P_{dp} – доцільність радіоелектронного придушення;

P_{in} – ймовірність наявності вільного передавача завад.

Тоді з урахуванням специфіки вогневого придушення P_{vp} запишеться так:

$$P_{vp} = P_{irp} P_{ivd} P_{im} P_{dv} P_{ivu}, \quad (2)$$

де P_{irp} – ймовірність розкриття лінії зв'язку;

P_{ivd} – ймовірність виявлення джерела випромінювання;

P_{im} – ймовірність визначення місцеположення станції;

P_{dv} – доцільність прийняття рішення на вогневе ураження.

P_{ivu} – ймовірність наявності вільних засобів вогневого ураження.

У свою чергу відомо, що ймовірність визначення місцеположення станції випромінювання має вигляд:

$$P_{im} = P_{kp} P_{pel} P_{rv}, \quad (3)$$

де P_{kp} – ймовірність проходження команди на пеленгування;

P_{pel} – ймовірність зняття пеленгів на станцію, що працює не менше, ніж двома пеленгаторами;

P_{rv} – ймовірність роботи на випромінювання станції, яка пеленгується.

Розкриємо складову P_{pel} більш детально. Як визначено [5] з основ застосування радіотехнічної розвідки ймовірність зняття пеленгів має певну кількість відомих складових таких, як

$$P_{pel} = \prod_{j=1}^m P_j, \quad j=1, 2, \dots, m.$$

$$\text{В свою чергу ймовірність } P_j = 1 - e^{-\frac{\Delta f_p T_n}{\Delta f T_c}}.$$

Доцільність придушення противником (як вогневого так, і радіоелектронного) залежить від оперативної обстановки, розвідувальної цінності лінії зв'язку та можливості її фізичного знищення. Тому в загальному випадку величину ймовірності P_{cp} аналітично визначити важко. Виходячи із врахування максимальних можливостей противника по РЕП і ВП, можна представити $P_{dp} = P_{dv} = 1$. Із цих же міркувань можна прийняти $P_{in} = P_{ivu} = 1$. Припустимо, що розкриті та запеленговані радіозасоби найбільш важливих об'єктів зв'язку (ПУ ОТУ, бригади, БТГ і т.д.), у відношенні яких противнику потрібне гарантоване запобігання передачі повідомлень одночасно вогневим і радіоелектронним придушенням (тобто $P_{in} = 1$). Тоді ймовірність прийняття

рішення на вогневе придушення, через імовірність прийняття рішення на радіоелектронне придушення, запишеться як:

$$P_{\text{вп}} = P_{\text{рп}} P_{\text{івд}} P_{\text{ім}}. \quad (4)$$

Надійність зв'язку по завмиранням залежить від рівня завад, від енергетичних характеристик, природи і статистики каналу, тому слід враховувати її не в обмеженнях, а в безпосередньому зв'язку з поведінкою комплексу радіоелектронного придушення противника [4]. Повільні завмирання, які найважче влаштувати, визначені змінами середовища поширення радіохвиль, відхиленнями коефіцієнтів підсилення антен і потужності передавальних пристроїв від номінальних значень та іншими випадковими факторами, призводять до того, що потужність сигналу й потужність навмисної завади на вході приймача мають випадковий характер і незалежні. Тут без деталізації аналітичного взаємозв'язку вважатимемо, що відношення потужності сигналу до потужності навмисної завади кількісно входить у ймовірність енергетичного придушення ($P_{\text{еп}}$).

Відповідно ймовірність надійності зв'язку по завмиранням при прийнятті противником рішення на РЕП ($P_{\text{зрп}}$) можна виразити через імовірність енергетичного придушення при ймовірності збігу часових інтервалів випромінювання сигналу і впливу навмисної завади:

$$P_{\text{зрп}} = 1 - P_{\text{еп}} P_{\text{л}}, \quad (5)$$

Будемо тут також припускати незастосування тих видів вогневого впливу, які можуть впливати на надійність по завмиранням. Уведемо наступні позначення:

$P_{\text{ф}}$ – ймовірність функціонування лінії зв'язку;

$P_{\text{п}} = 1 - P_{\text{ф}}$ – ймовірність простою лінії;

$P_{\text{т}}$ – технічна надійність;

$P_{\text{фоп}}$ – ймовірність виживання при вогневому придушенні;

$P_{\text{рп/вп}}$ – ймовірність прийняття рішення на радіопридушення при прийнятому рішенні на вогневе придушення (з огляду на викладене вважаємо $P_{\text{рп/оп}} = 1$);

$P_{\text{рп/вп}} - P_{\text{рп/вп}}$ – ймовірність прийняття рішення на радіопридушення при неприйнятому рішенні на вогневе придушення;

$1 - P_{\text{вп}}$ – ймовірність неприйняття рішення противником на вогневе придушення;

$1 - P_{\text{рп}}$ – ймовірність неприйняття на радіопридушення

$1 - P_{\text{рп/вп}}$ – ймовірність неприйняття противником рішення на радіоелектронне придушення та одночасно – неприйняття рішення на вогневе придушення

За умови того, що завадами придушуються все розкриті об'єкти, а вогневим ураженням – найбільш важливі за рішенням командира, то можна записати:

$$P_{\text{рп/вп}} = P_{\text{рп/вп}}. \quad (6)$$

Тепер можна записати співвідношення для імовірності функціонування в різних типових ситуаціях.

1) При не зіткненні з противником, коли $P_{\text{вп}} = P_{\text{рп}} \equiv 0$, маємо:

$$P_{\text{ф}} = P_{\text{т}} = P_{\text{з}}, \quad (7)$$

2) Перед початком бойових дій, коли $P_{\text{вп}} \equiv 0$, $P_{\text{рп}} \geq 0$, отримуємо

$$(P_{\text{рп/вп}} = P_{\text{рп}})$$

$$P_{\text{ф}} = P_{\text{т}} [P_{\text{рп}} P_{\text{зрп}} + (1 - P_{\text{рп}}) P_{\text{з}}]$$

Безумовно, що $P_{\text{зрп}} \leq P_{\text{з}}$.

3) У разі, коли противник застосовує або вогневе, або радіопридушення, тобто коли $P_{\text{оп/рп}} \equiv 0$, то можемо записати

$$P_{\phi} = P_{\tau} P_{\text{вп}} P_{\text{фоп}} P_3 + P_{\tau} (1 - P_{\text{оп}}) [P_{\text{рп/вп}} P_{\text{зрп}} + (1 - P_{\text{рп/вп}}) P_3] \quad (9)$$

Якщо тепер припустити, що один із способів придушення (вогневе або радіоелектронне) застосовується обов'язково, тобто $P_{\text{оп}} + P_{\text{рп}} \equiv 1$, звідки $P_{\text{рп/оп}} = 1$, то отримуємо:

$$P_{\phi} = P_{\tau} P_{\text{вп}} P_{\text{фоп}} P_3 + P_{\tau} (1 - P_{\text{вп}}) P_{\text{зрп}} \quad (10)$$

4) У загальному випадку довільної залежності між $P_{\text{оп}}$ і $P_{\text{рп}}$ отримуємо:

$$P_{\phi} = P_{\tau} P_{\text{вп}} P_{\text{фоп}} [P_{\text{рп/оп}} P_{\text{зрп}} + (1 - P_{\text{рп/вп}})] + P_{\tau} (1 - P_{\text{вп}}) [P_{\text{рп/вп}} P_{\text{зрп}} + (1 - P_{\text{рп/вп}}) P_3] \quad (11)$$

Якщо лінія зв'язку абсолютно живуча ($P_{\text{фо}} \equiv 1$) і рішення на радіопридушення приймається незалежно від рішення на вогневе придушення ($P_{\text{рп/вп}} \equiv P_{\text{рп/вп}} = P_{\text{рп}}$), то із (11) отримаємо:

$$P_{\phi} = P_{\tau} [P_{\text{рп}} P_{\text{зрп}} + (1 - P_{\text{рп}}) P_3] \quad (12)$$

Якщо лінія зв'язку абсолютно завадостійка ($P_{\text{зрп}} \equiv P_3$), то при цій же умові ($P_{\text{рп/оп}} \equiv P_{\text{рп/вп}} = P_{\text{рп}}$) із (11) отримуємо:

$$P_{\phi} = P_{\tau} P_3 [P_{\text{вп}} P_{\text{фоп}} + (1 - P_{\text{вп}})] = P_{\tau} P_3 [1 - P_{\text{вп}} (1 - P_{\text{фоп}})] \quad (13)$$

Розглянемо детальніше другий випадок. Надійність по завмиранням P_3 у порівнянні з надійністю по завмиранням в умовах навмисних завад можна припустити як така, що наближається до одиниці. Після розкриття дужок і заміни $P_{\text{зрп}}$ на (7), отримаємо

$$P_{\phi} = P_{\tau} P_3 - P_{\tau} P_{\text{рп}} P_{\text{еп}} P_{\text{т}} \quad (14)$$

На практиці частіше всього при оцінці якості лінії зв'язку використовують імовірність (коефіцієнт) простою $P_{\text{п}}$, який дорівнює $1 - P_{\phi}$. У (14) від'ємник $P_{\tau} P_3$, що характеризує надійність зв'язку при відсутності РЕП, приймемо рівним одиниці. Очевидно, $P_{\text{т}} = 1$. Звідси, як часткове рішення, отримуємо відоме раніше співвідношення:

$$P_{\text{п}} = P_{\text{рп}} P_{\text{еп}} P_{\text{т}}$$

Висновки. Запропоновані підходи доцільно використовувати при розробці стандартів, які визначають показники ефективності функціонування ліній зв'язку, а також для прийняття управлінських рішень щодо застосування ліній зв'язку в умовах вогневого та радіоелектронного придушення під час бойових дій.

Література

1. Боговик А.В. Теория управления в системах военного назначения / С.С.Загорулько, И.С.Ковальов, И.В.Котенко, А.В.Масановец / МО – М., 2001, 320 с.
2. Вентцель Е.С. Теория вероятностей: учебник – 12-е изд., стер. – М.: ЮСТИЦИЯ, 2018. – 658 с.
3. Казанцев О.Ю. Основы принятия решений та управлінська діяльність у військовій справі / Казанцев О.Ю., Гап'юк В.М., Мягков О.В., Каленський А.А. / ВІКНУ – К., 2003, 195 с.
4. Макаренко С.И., Иванов М.С., Попов С.А. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты. Монография. – СПб.: Свое издательство, 2013. – 166 с.: ил.
- С5. мирнов Ю.А. Радиотехническая разведка. – М.: Воениздат, 2001. – 456 с., ил.

ОГЛЯД МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ОБСЛУГОВУВАННЯ В СУЧАСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Козак А.Ю., Могилевич Д.І.

Інститут телекомунікаційних систем, КІП ім. Ігоря Сікорського

E-mail: anastasiia.kozak18@gmail.com

Overview of methods of service quality assurance in modern telecommunication networks

The basic methods of quality assurance in telecommunication networks have been monitored, and the optimal solutions for a high level of data transmission are given.

Проведено моніторинг основних методів забезпечення якості в телекомунікаційних мережах, наведено оптимальні рішення для високого рівня передачі даних.

Проблема забезпечення якості обслуговування (Quality of Service, QoS) в сучасних телекомунікаційних мережах (ТКМ) сьогодні є актуальною. Це обумовлено тим, що кожний тип трафіку потребує різних значень характеристик пропускної здатності мережі, продуктивності, надійності (одностороння затримка пакетів, варіації затримок пакетів, втрати пакетів, швидкість потоку, тощо) та вимог щодо його обслуговування. Домогтися одночасного дотримання всіх характеристик QoS для всіх видів трафіку досить складна задача. Одним з найбільш значущих факторів, що впливають на характеристики якості обслуговування, є рівень завантаження мережі трафіком або рівень використання пропускної здатності ліній зв'язку мережі. Основна ідея, що лежить в основі всіх методів підтримки характеристик QoS полягає в нерівномірному, тонкому перерозподілі наявної пропускної спроможності між трафіком різного типу відповідно до вимог додатків. Всі існуючі методи QoS в переважній більшості працюють на каналному та мережевому рівнях, де здійснюється управління чергами, контроль параметрів потоку трафіку, управління зворотнім зв'язком, боротьба з перевантаженнями, інжиніринг трафіку, кешування [1].

У методах забезпечення якості обслуговування використовуються різні механізми, спрямовані на зниження негативних наслідків перебування пакетів у чергах, зі збереженням, водночас, позитивної ролі черг. Більшість з них враховує й використовує у своїй роботі факт існування у мережі трафіка різного типу в тому сенсі, що кожний тип трафіка висуває різні вимоги до характеристик продуктивності й надійності мережі. Наприклад, трафік перегляду веб-сторінок малочутливий до затримок пакетів і не вимагає гарантованої пропускної здатності мережі, але чутливий до втрат пакетів; водночас голосовий трафік дуже чутливий до затримок пакетів, вимагає

гарантованої пропускної здатності мережі, але може «терпіти» втрату невеликого відсотка пакетів без значного збитку для якості (втім, остання властивість багато в чому залежить від використовуваного методу кодування голосового сигналу)[1].

Методи QoS засновані на тонкому перерозподілі наявної пропускної здатності між трафіком різного типу відповідно до вимог додатків. Зрозуміло, що ці методи ускладнюють мережне устаткування, оскільки означають необхідність знання вимог усіх класів трафіка, уміння їх класифікувати й розподіляти пропускну здатність мережі між ними. Остання властивість зазвичай досягається за рахунок використання декількох черг пакетів для кожного вихідного інтерфейсу комунікаційного устаткування замість однієї черги; при цьому в чергах застосовують різні алгоритми обслуговування пакетів, чим і досягається диференційоване обслуговування трафіка різних класів. Тому, методи QoS часто асоціюються з технікою керування чергами[1].

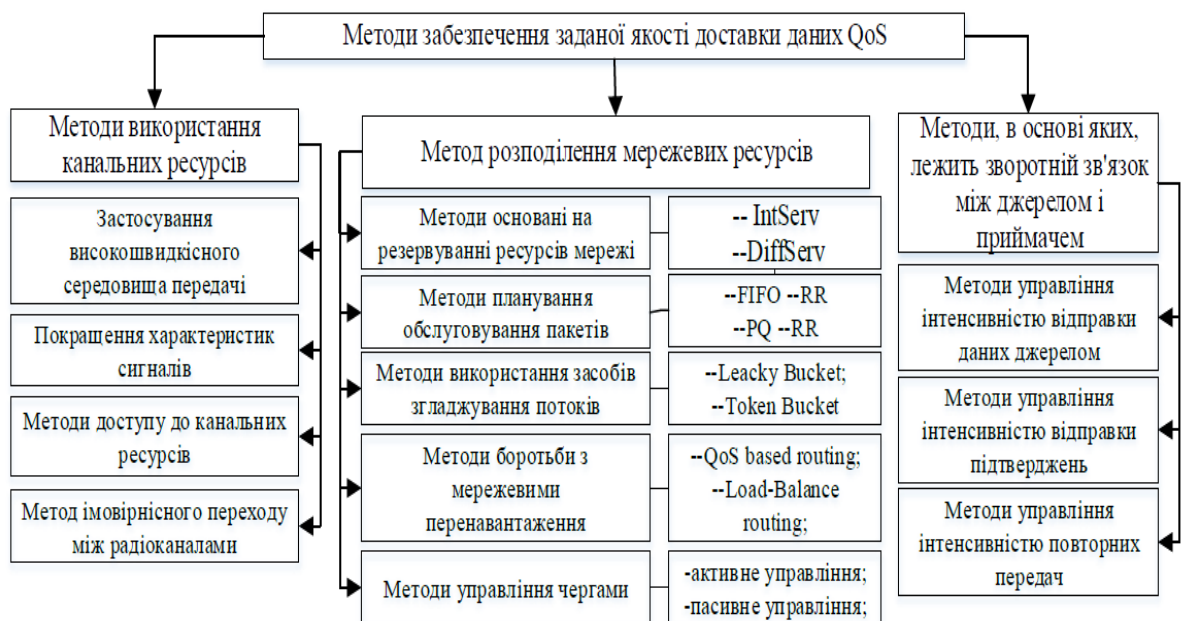


Рис. 1. Методи забезпечення якості обслуговування [2].

Крім власне техніки організації черг, до методів QoS належать методи контролю параметрів потоку трафіка, оскільки для гарантовано якісного обслуговування слід бути впевненими, що потоки, які обслуговуються, відповідають певному профілю. Ця група методів QoS отримала назву методів кондиціонування трафіка [1].

Особливе місце займають методи зворотного зв'язку, які призначені для повідомлення джерела трафіка про перевантаження мережі. Ці методи розраховані на те, що при отриманні повідомлення джерело знизить швидкість видачі пакетів у мережу й тим самим ліквідує причину перевантаження [1].

До методів QoS тісно примикають методи інжинірингу трафіка. Згідно з методами інжинірингу трафіка маршрути передачі даних керуються так, щоб забезпечити збалансоване завантаження усіх ресурсів мережі й виключити за

рахунок цього перевантаження комунікаційного устаткування і утворення довгих черг. На відміну від методів QoS у методах інжинірингу трафіка не

вдаються до організації черг з різними алгоритмами обслуговування на мережному устаткуванні. Водночас, у методах QoS у їхньому традиційному розумінні не використовують такий потужний важіль впливу на раціональний розподіл пропускну здатності, як зміна маршрутів трафіка залежно від фактичного завантаження ліній зв'язку, що дозволяє легко відокремити методи QoS від методів інжинірингу трафіка. У наступній групі методів боротьба з перевантаженнями ведеться за рахунок зниження постійного навантаження на мережу. Тобто в цих методах проблема розглядається з іншого боку: якщо пропускну здатності мережі недостатньо для якісної передачі трафіка додатків, то чи не можна зменшити обсяг самого трафіка? Найочевиднішим способом зниження обсягу трафіка є його компресія. Існують й інші способи, які призводять до того самого результату. Наприклад, розміщення джерела даних ближче до його споживача (кешування даних)[1].

Висновки. На даний момент існує кілька варіантів реалізації QoS в мережах, але кожен з них має недоліки, тому необхідна розробка додаткових рішень надання необхідного рівня сервісу.

Розглянуті методи підтримки якості обслуговування мають і переваги і недоліки, але так як на даний час ще немає універсального рішення, яке може забезпечити найбільш достовірну передачу даних для кожного типу трафіка, то оптимальним рішенням буде одночасне використання декількох методів передачі даних.

Література

1. Е.М. Бовда, В.В. Сальник "Методи забезпечення якості обслуговування в сучасних телекомунікаційних мережах військового призначення" // Збірник наукових праць Харківського університету Повітряних Сил. - 2017. - № 2. - С. 85-94. - Режим доступу: http://nbuv.gov.ua/UJRN/ZKhUPS_2017_2_19.
2. Стрела Т.С , Романюк В.А. , Жук О.В., Олексенко В.П. "Аналіз методів підвищення та забезпечення якості обслуговування в безпроводових сенсорних мережах" Збірник наукових праць ВІТІ, 2018, Вип. 1.- С. 141–148. - Режим доступу: http://nbuv.gov.ua/UJRN/Znpviti_2018_1_19.
3. Кудзиновская И. П. "Анализ методов обеспечения качества обслуживания в высокоскоростных компьютерных сетях"//Проблеми інформатизації та управління, 1(23)'2008 - Режим доступу: <http://masters.donntu.org/2010/fkita/tishenko/library/article1.htm>.

АНАЛІЗ ВИКОРИСТАННЯ ПРОТОКОЛІВ IPSEC ТА SSL В КОРПОРАТИВНИХ МЕРЕЖАХ

Турчин Я. В., Кононова І.В.

*Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: turchyn_v@ukr.net*

Analysis of the use of IPsec and SSL in corporate networks

The analysis of the use of IPsec and SSL protocols to improve the level of information security in corporate networks is conducted. Based on the analysis, the main advantages and disadvantages of these protocols are identified, the main problems of providing information security of the network during the construction of the virtual network are identified.

Проблема захисту інформації в сучасних інформаційних системах від несанкціонованого доступу та спотворення на даний є актуальною проблемою. При появі загроз, пов'язаних з можливістю втрати, спотворення, розкриття конфіденційних даних і витоку стратегічно важливої інформації, організація або держава в цілому може втратити не тільки статки, але і репутацію на політичному та економічному рівні.

Домогтися високого ступеня захищеності можна тільки при використанні передових технологій захисту мережі передачі даних. На даний час одним із засобів забезпечення безпеки в мережі Інтернет є використання протоколів захищеної передачі даних, а саме:

SSL (Secure Sockets Layer — рівень захищених сокетів);

IPsec (IP Security — набір протоколів для забезпечення захисту даних, що передаються за допомогою протоколу IP).

Розглянемо детальніше можливості, переваги та недоліки цих протоколів.

SSL — це протокол забезпечення безпеки, який використовує сучасний метод шифрування для отримання і відправки конфіденційної інформації по Інтернету. Він працює шляхом створення захисного каналу між браузером користувача і сайтом, який користувач збирається відвідати. Будь-яка інформація відправлена по цьому каналу шифрується з однієї сторони і розшифровується отримувачем з іншої сторони. Таким чином, якщо навіть хтось зможе заволодіти цією інформацією, він не зможе її розшифрувати [2].

Однак даний сертифікат передбачений тільки для обміну даними між користувачами, які дають підтвердження SSL сертифікатам, а самопідписані сертифікати забезпечують тільки безпечну передачу даних, однак не дають підтвердження про компанію. Також самопідписані сертифікати часто використовують хакери, здійснюючи фішингові атаки, перенаправляючи користувачів на сайт зі схожою адресою.

Проаналізувавши сучасний стан захисту інформації за допомогою протоколу SSL та виділивши його основні недоліки переходимо до розгляду протоколу IPsec. При аналізі реалізації віртуальних приватних мереж протокол IPsec суттєво домінує та має ряд переваги у порівнянні з SSL (рис. 1).

Технологія	IPSec	SSL
Апаратна залежність	Так	Так
Код	Не потребує змін для додатків. Може вимагати доступ вихідного коду стека TCP/IP.	Потрібні зміни в додатках. Можуть знадобитися нові DLL або доступ до вихідного коду додатків.
Захист	IP-пакет цілком. Включає захист для протоколів верхніх рівнів.	Тільки рівень додатків
Фільтрація пакетів	Заснований на автентифікованих заголовках, адреси відправника і одержувача, і т.д. Проста і дешева, підходить для маршрутизаторів.	Заснована на вмісті і семантиці високого рівня. Більш складна.
Платформи	Будь-які системи, включаючи маршрутизатори.	В основному, кінцеві системи (клієнти/сервери), а також брандмауери.
Firewall/VPN	Весь трафік захищений	Захищений тільки трафік рівня додатків
Прозорість	Для користувачів і додатків	Тільки для користувачів

Рис. 1. Порівняльна характеристика IPSec та SSL.

Протокол IPSec - це набір протоколів Internet Engineering Task Force (IETF) між двома точками зв'язку в мережі IP, які забезпечують автентифікацію даних, цілісність та конфіденційність. Він також визначає зашифровані, розшифровані та автентифіковані пакети. У ньому визначені протоколи, необхідні для безпечного обміну та управління ключами.

Протокол IPSec надає можливість виконувати наступні дії: - шифрування даних додаткового рівня; - забезпечення безпеки маршрутизаторів, що надсилають дані про маршрутизацію через загальнодоступну мережу Інтернет; - забезпечення автентифікації без шифрування; - захист мережових даних, шляхом побудови схеми тунелю IPSec, в якому всі дані передаються між двома кінцевими точками, шифруються, як при підключенні до віртуальної приватної мережі (VPN).

Тунельний режим несе в собі шифрування всього пакету, навіть включаючи заголовок мережового рівня. Тунельний спосіб застосовують у випадку необхідності приховування обміну інформацією організації з навколишнім середовищем. При цьому, адресне поле заголовка мережового рівня пакета, котрий використовує тунельний режим, заповнюється міжмережовим екраном організації і не несе в собі інформації про конкретного відправника пакета даних. При передачі даних із зовнішнього середовища у внутрішню мережу організації в якості кінцевої адреси використовується мережева адреса міжмережового екрана. Після розшифрування екраном початкового заголовка мережового рівня пакет відправляється отримувачу.

Особливістю IPSec є те, що він реалізується на мережевому (третьому) рівні, доповнюючи його таким чином, щоб для подальших рівнів все відбувалося непомітно. Але, основна складність полягає в тому, що в процесі встановлення з'єднання двом учасникам захищеного каналу необхідно

узгодити досить велику кількість параметрів. І саме вони мають аутентифікувати один одного, згенерувати і обмінятися ключами, а також домовитися, які протоколи вони будуть використовувати для подальшого шифрування даних.

Саме з цієї причини IPsec і складається зі стека протоколів, обов'язок, яких полягає в тому, щоб забезпечити встановлення захищеного з'єднання, його роботу та управління ним. IPsec підтримує два типи схем управління ключами, за допомогою яких учасники можуть узгодити параметри сеансу. Із версією IP, IPv4, можуть бути використані або ISAKMP, або ж Simple Key Management for Internet Protocol.

З погляду політики безпеки при VPN-з'єднання використання протоколу ISAKMP (Internet Security Association and Key Management Protocol) є надійнішим, це протокол узгоджує поновлення політик безпеки (SA) між учасниками віртуального з'єднання. Саме використання цього протоколу передбачає нова версія IP, IPv6, хоча не виключається можливість використання SKIP.

Необхідно зазначити, що протокол IPsec є безпечним протоколом при наданні захисту в мережах з пакетною передачею даних, але існує думка, що присутня складність роботи і надмірність протоколу ускладнює його масове використання та набір протоколів вимагає доопрацювання.

У цій статті було розглянуто деякі основні моменти, що стосуються протоколу мережевої безпеки IPsec. Можна зробити висновок, що протокол IPsec домінує в більшості реалізацій віртуальних приватних мереж.

Отже, на основі аналізу можна зробити висновок, що на сьогоднішній день найбільш надійними являються протоколи IPsec та SSL, але пріоритет їх використання для побудови VPN залежить від конкретних критеріїв (необхідний тип доступу для користувачів, рівень мережевої безпеки, рівень захист даних, необхідність масштабованості мережі в майбутньому). Розглянувши основні моменти, які стосуються протоколу мережевої безпеки IPsec можна відмітити, що даний протокол домінує в більшості реалізацій віртуальних приватних мереж.

Метою подальших досліджень буде удосконалення методів побудови захищених з'єднань за допомогою протоколу IPsec за схемами “точка-точка” і “мережа-мережа”.

Література

1. IPsec – протокол защиты сетевого трафика на IP-уровне. – IXBT.com. – Електронний ресурс. Режим доступу: <https://www.ixbt.com/comm/ipsecure.shtml>.
2. Почему SSL? Три преимущества использования SSL- сертификата. – HOSTINGER.com – Електронний ресурс. Режим доступу: <https://www.hostinger.com.ua/rukovodstva/ssl-tri-preimuschestva-ispolzovania-ssl-certificata/>
3. IP security (IPsec). – GEEKSFORGEES.org. – Електронний ресурс. Режим доступу: <https://www.geeksforgeeks.org/ip-security-ipsec/>
4. IPsec проткол. – CRIBS.me. – Електронний ресурс. Режим доступу: <https://cribs.me/zashchita-informatsii-zi/ipsec-protokol>.
5. IP security (IPsec). – BMSTU.wiki. – Електронний ресурс. Режим доступу: [https://ru.bmstu.wiki/IPsec_\(IP_Security\)](https://ru.bmstu.wiki/IPsec_(IP_Security)).

ГРАНИЧНЕ ЗНАЧЕННЯ БЛОКУ КОДІВ ХЕМІНГА ПРИ ЗАДАНИХ ВИМОГАХ ЩОДО ДОСТОВІРНОСТІ ПРИЙОМУ

Уривський Л. О., Корнієнко А. А.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: leonid_uic@ukr.net, f.c.otradniy@gmail.com

Hemming code block limit at the given requirements for reception reliability

The basic parameters of the Hamming codes are summarized. A four-dimensional view of the parameters of the Hamming codes and their relationship is considered to understand the length of the block to select the code based on the specified requirements for reliability of reception.

Найбільш відомий з перших коригуючих кодів – код Хемінга, який здатний виправляти одиничну помилку та знаходити подвійну не залежно від довжини блоку коду. Коди Хемінга є досконалими, тобто за своєю структурою співпадаючими з границею Хемінга [1].

Відповідно до корегуючих здатностей, коди Хемінга мають фіксовані параметри відстані Хемінга d , кількості виправлених помилок t та кількості виявлених помилок s : ($d = 3; t = 1; s = 2$) – незалежно від довжини блоку n .

Позитивна риса кодів Хемінга полягає в тому, що при рості числа символів у блоці n , зростає швидкість кодування R (табл.1; рис.1):

Таблиця 1: Швидкість кодів Хемінга.

Код Хемінга (n, k) $d_{min} = 3$	$R = k/n$
(7,4)	0,571
(15,11)	0,733
(31,26)	0,839
(63,57)	0,905
(127,120)	0,945
(255,247)	0,969
(511,502)	0,982
(1023,1013)	0,990

Отже, частка інформаційних символів k в суцільному блоці із n символів зростає.

Проте, при цьому потрібно враховувати, що при збільшенні числа символів у блоці може збільшитись кількість помилок, які попадуть у цей блок, а виправна здатність коду Хемінга стала ($t = 1$).

Отже, об'єктом дослідження є з'ясування динаміки обох процесів при зростанні довжини блоку n : зростання швидкості кодування R та зростання уразливості відповідного блоку – при сталій енергетиці каналу зв'язку.

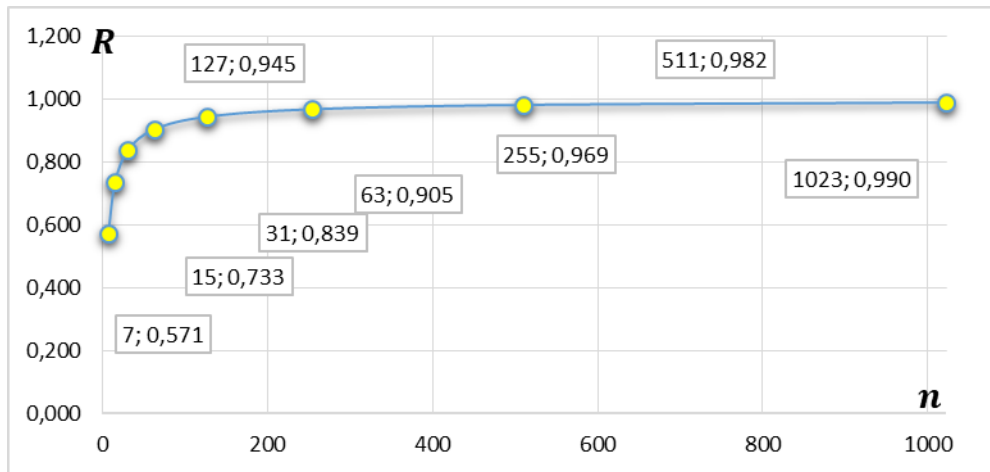


Рис. 1. Залежність швидкості коду від довжини блоку.

Нехай задані вимоги до достовірності прийому символів джерела на вході пристрою одержувача: $P_6 = 10^{-6}$. Розглянемо, якою має бути ймовірність помилки на символ на виході каналу зв'язку $p_{\text{ош}}$, в залежності від довжини блоку коду n , щоб досягнути потрібної достовірності після корегування за рахунок виправлення t помилок ($m = t = 1$) у блоці довжиною n . Для цього виведемо рівняння для вірогідності $p(m, n)$ виникнення t помилок у блоці довжиною n через біноміальний розподіл [1], та властивість нормування (1):

$$\sum_{m=0}^n p(m, n) = 1 \quad (1)$$

$$P_6 \leq \sum_{m=t+1}^n p(m, n) \quad (2)$$

Формула (2) визначає ймовірність P_6 помилкового прийому кодового слова на виході декодера, яку декодер виправити не може і яка являє собою суму ймовірностей виникнення $t + 1, t + 2, \dots, n$ помилок. Тоді, щоб знайти ймовірність правильного прийому, наприклад, для коду (7,4), переробимо біноміальний розподіл, який використовували вище, а саме границю ймовірності правильного прийому $P_{\text{пп}}$ [2]:

$$\begin{aligned}
 P_{\text{пп}} &= \sum_{m=0}^{m < t+1} C_n^m p_{\text{ош}}^m (1 - p_{\text{ош}})^{n-m} = \\
 &= C_7^0 p_{\text{ош}}^0 (1 - p_{\text{ош}})^{7-0} + C_7^1 p_{\text{ош}}^1 (1 - p_{\text{ош}})^{7-1} = 1 - 10^{-6}
 \end{aligned} \quad (3)$$

Вирішивши дане рівняння (3), отримуємо значення ймовірності помилки на символ на виході каналу $p_{\text{ош}} = 2,18 \cdot 10^{-4}$. Виконавши дану процедуру для інших кодів Хемінга занесемо дані у таблицю (табл. 2):

Таблиця 2: Ймовірність помилкового прийому.

Код Хемінга (n, k) $d_{min} = 3$	$p_{ош}$
(7,4)	$2,18 \cdot 10^{-4}$
(15,11)	$9,76 \cdot 10^{-5}$
(31,26)	$4,64 \cdot 10^{-5}$
(63,57)	$2,26 \cdot 10^{-5}$
(127,120)	$1,12 \cdot 10^{-5}$
(255,247)	$5,56 \cdot 10^{-6}$
(511,502)	$2,77 \cdot 10^{-6}$
(1023,1013)	$1,38 \cdot 10^{-6}$

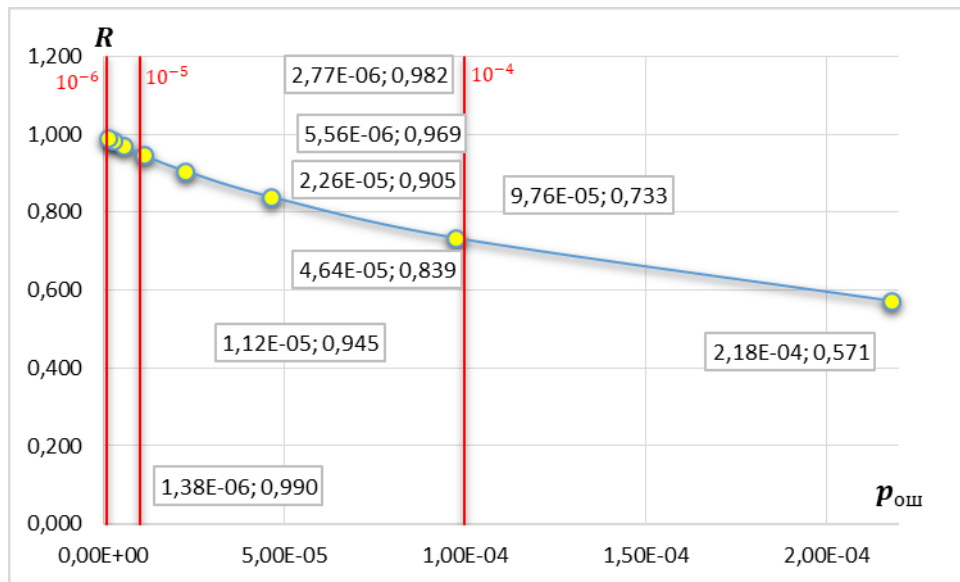


Рис. 2. Залежність ймовірності помилкового прийому від швидкості коду.

Результати дослідження (рис.2) показали, що:

- досконалий код Хемінга втрачає корисні корегуючі властивості з ростом довжини блоку n , тому що його виправна здатність не змінюється, а кількість виникаючих помилок при цьому зростає;
- в даному випадку доречно використовувати коди Хемінга до граничного значення довжини блоку коду 1023, опираючись на задані вимоги, оскільки подальше збільшення довжини блоку вже не має сенсу, тому що задана достовірність має місце й без кодування.

Література

1. Основи теорії телекомунікацій / Підручник / За заг. ред. проф. Ільченка М.Ю. – К.: 2010. – ICCЗІ НТУУ «КПІ» – с.786, іл.
2. Art of Doing Science and Engineering: Learning to Learn / Richard R. Hamming. - К.: 2003. – CRC Press – с.376.

АНАЛІТИЧНА МОДЕЛЬ БЕЗПРОВОДОВОГО КАНАЛУ СЕНСОРНОЇ МЕРЕЖІ В УМОВАХ ЗАВМИРАНЬ І ВИПАДКОВОГО РОЗКИДУ ПАРАМЕТРІВ ПРИЙМАЛЬНО-ПЕРЕДАВАЧІВ

Новіков В.І.

*Інститут телекомунікаційних систем КІП ім. Ігоря Сікорського,
Україна*

E-mail: novikov1967@ukr.net

Model wireless channel sensor networks in conditions of fading and random variation of parameters transceiver

An analytical model of the wireless channel sensor network in fading and random scatter parameters transceivers. The new model takes into account the anisotropy of the path loss and obstacles in the signal path.

Безпроводова сенсорна мережа (БСМ) - це розподілена мережа великого числа (до декількох десятків тисяч) автономних сенсорних вузлів, здатних обмінюватися повідомленнями і ретранслювати їх по безпроводовим каналам зв'язку. У більшості робіт робота БСМ розглядається з використанням спрощеної моделі безпроводового каналу зв'язку, згідно якої повідомлення успішно приймається тільки за умови, що відстань між передавачем і приймачем менше деякого фіксованого радіуса радіозв'язку τ . В іншому випадку повідомлення ігнорується.

Проте численні експериментальні дослідження характеристик малопотужних безпроводових каналів зв'язку показали, що діапазон прийому умовно розділений на 3 області: область надійного прийому, перехідна область та область відсутності зв'язку. В області надійного прийому з'єднання забезпечують високу та стабільну якість зв'язку, в той час як перехідна область відрізняється значною варіацією та асиметрією показників надійності.

Аналіз досліджень і публікацій [1-3] показує, що перехідна область може мати істотний негативний вплив на характеристики верхніх мережевих рівнів, в першу чергу - на ефективність маршрутизації. Наприклад, в [3] виявлено, що при нерівномірності властивостей каналу в різних напрямках передачі географічна маршрутизація (наприклад, GPSR) демонструє гірші характеристики, ніж традиційна маршрутизація реактивного типу (наприклад, AODV і DSR), яка опирається виключно на топологію мережі і довжину найкоротших шляхів в кількості проміжних сполучень.

В доповіді пропонується аналітична модель радіочастотного каналу зв'язку в умовах завмирань і випадкового розкиду параметрів приймально-передавачів. Для вирішення завдання розроблено модель втрат в канали в умовах впливу завмирань. При цьому враховано вплив анізотропії та вплив перешкод. При створенні моделі приймально-передавача визначено відношення сигнал/ шум та імовірність успішного прийому пакета.

У більшості практичних додатків БСМ використовуються в умовах впливу ефектів затінення (завмирань), тому застосуємо загальноприйнятну модель логарифмічно нормального розподілу втрат в тракці:

$$PL(d) = PL(d_0) + 10\alpha \lg \left(\frac{d}{d_0} \right) + X_{\sigma_{ch}} = \overline{PL}(d) + X_{\sigma_{ch}}, \text{дБ}, \quad (1)$$

де

d - відстань між передавачем і приймачем, м;

d_0 - еталонна відстань, м;

α - показник ступеня втрат в тракці;

$\overline{PL}(d)$ - середні втрати в тракці на відстані d , дБ;

$X_{\sigma_{ch}}$ - випадкова Гауссова змінна з нульовим середнім і дисперсією $X_{\sigma_{ch}}^2$, дБ.

Саме модель логарифмічно нормального розподілу втрат в тракці найбільш часто використовується в роботах по БСМ і яка показала свою спроможність в численних експериментальних дослідженнях.

Для обліку анізотропії діаграм спрямованості антен використовуємо модель нерівномірності приймально-передавачів RIM (Radio irregularity model) [3, 4], в якій введено поняття ступеня нерівномірності DOI (Degree of irregularity) як максимальне відносне відхилення величини загасання при одиничній зміні напрямку передачі.

Припускаючи розміщення вузлів на площині і приймаючи як одиницю зміни напрямку передачі 1 кутовий градус, можна задати 360 коефіцієнтів $\{K_i\}_{i=0}^{359}$, що відображають відмінності втрат у різних напрямках. Тоді для i -го напрямку коефіцієнт дорівнює

$$K_i = \begin{cases} 1, & \text{при } i = 0; \\ K_{i-1} \pm R_w \times DOI, & \text{при } 0 < i < 360, \end{cases} \quad (2)$$

де R_w - випадкова величина, розподілена за законом Вейбулла.

При цьому для набору коефіцієнтів $\{K_i\}_{i=0}^{359}$ повинна виконуватися гранична умова $|K_{i-1} - K_{359}| \leq DOI$

Вплив заздалегідь відомих перешкод (наприклад, стін) між заданими вузлами v та w може бути врахований введенням у вираз (1) додаткового доданка Ω_{vw} , що характеризує сумарне загасання (в дБ), яке вносять перешкоди на шляху проходження сигналу між вузлами v та w .

Таким чином, загальна формула втрат в тракці між вузлами v та w має вигляд

$$PL_{vw}(d) = K_{v,i} K_{w,j} [\overline{PL}(d) + \Omega_{vw}] + X_{\sigma_{ch}}, \text{дБ}, \quad (3)$$

Вираз (3) враховує ефекти затінення, анізотропію втрат і перешкоди між вузлами.

Відзначимо, що згідно (3) для двох вузлів v і w втрати в тракці однакові в обох напрямках передачі, але можуть відрізнятися для іншої пари вузлів, що знаходиться на тій же відстані відносно один одного, тобто в загальному випадку для $\forall v, w, u \in V$ мають місце вирази:

$$\begin{aligned} PL_{vw}(d) &= PL_{wv}(d), \\ PL_{vw}(d) &\neq PL_{vu}(d). \end{aligned}$$

Параметри реальних приймально-передавачів мають випадкові відхилення від номінальних значень, що викликано як технологічним процесом виробництва інтегральних мікросхем та інших компонент радіопристроїв, так і особливостями апаратної реалізації вузлів. Розкид значень вихідної потужності P_t і рівня шуму P_n приймально-передавачів підпорядковуються нормальному закону розподілу, при цьому в загальному випадку P_t і P_n є залежними випадковими величинами для конкретного екземпляра приймально-передавача інтегрального виконання. Тоді розподіл пар значень P_t і P_n описується наступним законом:

$$\begin{bmatrix} P_t \\ P_n \end{bmatrix} \sim \mathcal{N} \left(\begin{bmatrix} \bar{P}_t \\ \bar{P}_n \end{bmatrix}, \Sigma_{hw} \right), \quad (4)$$

де

$\bar{P}_t$ - середнє (номінальне) значення вихідної потужності передавача, дБм;

$\bar{P}_n$ - середнє (номінальне) значення рівня шуму приймача, дБм;

Σ_{hw} - коваріаційна матриця вектора $[P_t, P_n]^T$ виду

$$\Sigma_{hw} = \begin{bmatrix} \sigma_t^2 & cov(P_t, P_n) \\ cov(P_n, P_t) & \sigma_n^2 \end{bmatrix}.$$

При передачі даних від вузла v до вузла w на відстань d відношення сигнал/шум (ВСШ) на вході приймача вузла w дорівнює:

$$\gamma_{vw}(d) = P_{v,t} - PL_{vw}(d) - P_{w,n}, \text{ дБ}, \quad (5)$$

де

$P_{v,t}$ - вихідна потужність передавача вузла v , дБм;

$P_{w,n}$ - рівень шуму приймача вузла w , дБм.

У формулі (5) використовуються значення вихідної потужності та рівня шуму для різних вузлів, тому вони є незалежними щодо один одного випадковими величинами з розподілами $\mathcal{N}(\bar{P}_t, \sigma_t^2)$ та $\mathcal{N}(\bar{P}_n, \sigma_n^2)$ відповідно. Отже, попередній вираз можна звести до наступного вигляду:

$$\gamma_{vw}(d) = \bar{P}_t - PL_{vw}(d) - \bar{P}_n + \mathcal{N}(0, \sigma_{hw}^2), \text{ дБ}, \quad (6)$$

де $\sigma_{hw}^2 = \sigma_t^2 + \sigma_n^2$.

Випадкова складова $\mathcal{N}(0, \sigma_{hw}^2)$ у виразі (6) вносить асиметрію в якість зв'язку між вузлами, тобто в загальному випадку $\gamma_{vw}(d) \neq \gamma_{wv}(d)$.

Залежність ймовірності бітової помилки (Bit error rate (BER) від значення ВСШ γ визначається типом маніпуляції. Як приклад, розглянемо фізичний рівень стандарту IEEE 802.15.4 та використаємо функцію із специфікації стандарту [5]:

$$\beta(\gamma) = \frac{8}{15} \times \frac{1}{16} \times \sum_{k=2}^{16} (-1)^k C_{16}^k \exp \left[20 \left(\frac{1}{k} - 1 \right) 10^{\gamma/10} \right], \quad (7)$$

де

$C_{16}^k = \frac{16!}{k!(16-k)!}$ - біноміальний коефіцієнт;

γ - відношення сигнал/шум, дБ.

Імовірність успішного прийому пакета (коефіцієнт прийнятих пакетів - Packet reception rate (PRR)) довжиною L байт дорівнює

$$\psi(\beta, L) = (1 - \beta)^{8L} \quad (8)$$

Вираз (8) записано у припущенні про незалежність і рівномірність бітових помилок, а також про відсутність спеціального кодування двійкових символів, що вірно для приймально-передавачів стандарту IEEE 802.15.4. Якщо ж використовується яка-небудь схема кодування, то залежність пакетної помилки від ймовірності бітової помилки може мати інший вигляд, але при цьому нижче наведені міркування залишаються в силі.

Таким чином, запропоновані вирази (3) - (8) являють собою модель безпроводового каналу зв'язку БСМ, що дозволяє розрахувати ймовірність успішного прийому пакетів в умовах завмирань і за наявності випадкових відхилень параметрів приймально-передавачів від номінальних значень. При типах маніпуляції і схемах кодування, відмінних від IEEE 802.15.4, змінюється тільки вид виразів (7) і (8).

Таким чином, запропоновано аналітичну модель безпроводового каналу БСМ в умовах завмирань і випадкового розкиду параметрів приймально-передавачів. Модель дозволяє врахувати ці ефекти при розробці та дослідженні алгоритмів функціонування БСМ з метою створення більш ефективних у реальних умовах експлуатації рішень, а також для отримання при імітаційному моделюванні більш адекватних оцінок. На відміну від моделі з робіт [6, 7] нова модель враховує анізотропію втрат в тракті і перешкоди на шляху проходження сигналу.

Література

1. Complex behavior at scale: an experimental study of low-power wireless sensor networks: Technical report 02-0013 / University of California (Los Angeles); D. Ganesan [et al.]. 2002. 11 p.
2. The mistaken axioms of wireless-network research: Technical report 2003-467 / Dartmouth College; Kotz D., Newport C, Elliott C 2003. 14 p.
3. Impact of radio irregularity on wireless sensor networks / G. Zhou [et al.] // Proceedings of the 2nd international conference on mobile systems, applications, and services. Boston (USA), 2004. P. 125-138.
4. Models and solutions for radio irregularity in wireless sensor network / G. Zhou [et al.] // ACM transactions on sensor networks. 2006. Vol. 2, no. 2. P. 221-262.
5. IEEE Std 802.15.4-2006. IEEE standard for local and metropolitan area networks. Part 15.4: wireless medium access control (MAC) and physical layer (PHY) specifications for low rate wireless personal area networks (LR-WPANs). New York (USA): IEEE Computer Society, 2006. 323 p.
6. Zuniga M., Krishnamachari B. Analyzing the transitional region in low power wireless links // Proceedings of the 1st annual IEEE communications society conference on sensor and ad hoc communications and networks. Santa Clara (USA), 2004. P. 517-526.
7. Zuniga M., Krishnamachari B. An analysis of unreliability and asymmetry in low-power wireless links // ACM transactions on sensor networks. 2007. Vol. 3, no. 2. P. 7.1-7.34.

ПОРІВНЯННЯ ЗАВАДОСТІЙКОСТІ ШИРОКОСМУГОВИХ ТА ВУЗЬКОСМУГОВИХ СИГНАЛІВ ЗВ'ЯЗКУ В УМОВАХ НИЗЬКОЇ ЕНЕРГЕТИКИ

Уривський Л.О., Шмігель Б.О.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: leonid_uic@ukr.net, bshmigel@gmail.com

Noise immunity comparison of narrowband and broadband signals in low energy conditions

In this paper considered a comparative analysis of the noise immunity of wideband and narrowband signals. The properties of broadband signals in low energy conditions are analyzed.

Стрімкий розвиток телекомунікаційних систем породжує необхідність забезпечення стійкого зв'язку в умовах низької енергетики ліній зв'язку, завад та багатопроменевого розповсюдження.

У вітчизняних та зарубіжних публікаціях достатньо досліджено окремо умови використання широкосмугових сигналів (ШСС) [1-3] але немає досліджень властивостей цих сигналів в умовах низької енергетики. До того ж, тематика досягнення необхідної достовірності в низькоенергетичних каналах не достатньо досліджена. Тому тема доповіді є актуальною.

Відомо, що ШСС можуть забезпечити високу достовірність прийому з невеликими коливаннями ймовірності помилок, в той час як при вузькосмугових сигналах (ВСС) іноді (при відсутності завад на даній частоті) достовірність зв'язку буде дуже високою, а іноді дуже низькою. Це обумовлено тим, що в смузі частот ВСС спектральна щільність перешкод може сильно флюктувати, а в смузі частот ШСС вона змінюється мало. З розширенням смуги відбувається усереднення діючих в цій смузі завад.

Метою доповіді є визначення властивостей ШСС на основі моделей оцінки якості каналів зв'язку, а також порівняння характеристик завадостійкості з ВСС за умов еквівалентної енергії сигналу.

Широкасмуговими сигналами (ШСС) називають такі сигнали, у яких добуток ширини їх спектра $\Delta F_{ШСС}$ на тривалість елементу сигналу $\tau_{ШСС}$ багато більше одиниці, тобто база сигналу B :

$$B = \Delta F_{ШСС} * \tau_{ШСС} \gg 1. \quad (1)$$

Частіше значення B досягає 1000 і більше. Головним чинником, заради якого може бути істотно збільшено базу сигналу B є підвищена прихованість системи із широкосмуговому сигналами.

За умов зберігання швидкості передавання символів інформації V_s та об'єму сигналу W_c , як незмінне значення добутку потужності сигналу P_c , тривалості інформаційного символу τ_s та смуги ΔF_c :

$$W_C = P_C * \tau_s * \Delta F_C, \quad (2)$$

параметри ШСС слід розглядати, як перерозподіл відповідних параметрів ВСС за рахунок скорочення елементу ШСС в n разів:

$$\tau_{ШСС} = \tau_s / n. \quad (3)$$

Відповідно, $\Delta F_{ШСС} \approx 1/\tau_{ШСС} = n * \Delta F_C$.

Отже, при цьому об'єм сигналу ШСС: $w_{ШСС} = P_C * \tau_{ШСС} * \Delta F_{ШСС} = w_C$, – є тотожним об'єму сигналу ВСС (2).

Результуюча енергія ШСС:

$$P_C * \tau_{ШСС} * n = P_C * \tau_s = E_C, \quad (4)$$

співпадає з енергією первинного ВСС, що визначає незмінність параметру h^2 при порівнянні завадостійкості ШСС та ВСС.

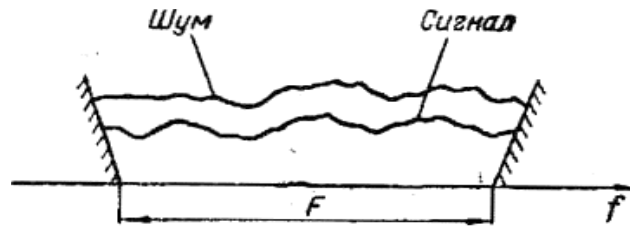


Рис. 1. Прийом ШСС при потужності сигналу, меншій від потужності флукуаційних перешкод у використовуваній смузі частот.

Розглянемо показники завадостійкості системи ШСС з активною паузою і протилежними сигналами, як одну із найбільш завадостійких [1].

Тоді вираз для залежності ймовірності помилки інформаційного біта p_b від відношення потужності сигнал/шум (параметра h^2) у автокореляційній системі з активною паузою і протилежними сигналами має вигляд [1]:

$$P_b(h^2) = \frac{1}{2} \left[1 - \Phi \left(\frac{h^2}{\sqrt{\frac{5h^4}{2FT} + 4h^2 + 2FT}} \right) \right]. \quad (4)$$

Для порівняння показників ШСС з показниками достовірності ВСС при побудови графіків для сигналу з фазовою маніпуляцією, скористаємося співвідношенням [4]:

$$P_{b\text{ PSK}}(h^2) = \frac{1}{2} [1 - \Phi(\sqrt{2h^2})]. \quad (5)$$

Відповідно до формул, побудуємо графіки залежності ймовірності бітової помилки p_b від енергетичного потенціалу в радіолінії h^2 .

Порівнюючи завадостійкість ШСС та ВСС, бачимо, що при однакових значеннях h^2 ВСС мають кращу завадостійкість в порівнянні з широкосмуговими. Наприклад, для забезпечення достовірності 10^{-6} для ФМ достатньо значення $h^2=10.5$ дБ.

Одночасно, із графіків (рис.2) видно, що при зростанні бази В,

необхідно збільшувати h^2 для досягнення еквівалентної достовірності сигналу.

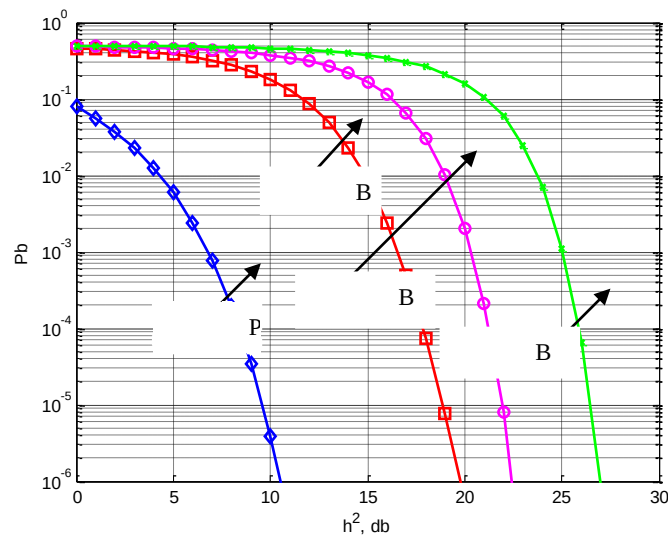


Рис. 2. Порівняння завадостійкості ШСС з активною паузою і протилежними сигналами та ВСС ФМ з еквівалентною потужністю.

Для широкосмугового сигналу для забезпечення достовірності 10^{-6} на виході декодера при $V=100$ необхідно забезпечити $h^2 = 19.8$ дБ, при $V=1000$ – $h^2 = 22.4$ дБ, а при $V=10000$ – $h^2 = 27$ дБ. Це пояснюється тим, що потужність завад в смузі частот F при використанні ШСС накопичується в цій смузі в V раз більше шумів в порівнянні зі смугою ВСС. Поряд з цим, ця закономірність витікає також із виразу (5).

Це визначає доцільність використання широкосмугових систем в тих випадках, коли швидкість передачі інформації не має вирішального значення, а прихованість системи або вірність прийому сигналів в умовах каналу з сильно змінними параметрами грає особливо важливу роль.

Висновки. Широкосмугові сигнали, попри деяких існуючих суджень, не забезпечують кращої достовірності і є виправданими в тих випадках, коли необхідно забезпечувати зв'язок в умовах впливу штучних перешкод з боку супротивника. Якщо ШСС має обмеження в ресурсі (обмежена енергія сигналу), то вони ведуть до втрати завадостійкості або розтрати ресурсу, коли є намагання відновити вихідну достовірність. Засобом, що дозволяє підвищити достовірність прийому є завадостійке кодування, однак декодер не може розрізняти спосіб обробки сигналу до його входу, тому при рівній енергетиці і однаковій швидкості символів джерела, ВСС мають перевагу і на цьому етапі обробки сигналів.

Література

1. Семенов А.М., Сикарев А.А. Широкополосная радиосвязь. – М.: Воениздат, 1970. – 280 с.
2. Варакин Л. Системы связи с шумоподобными сигналами. – М.: Радио и связь, 1985. – 384 с.
3. Мазурков М. Системы широкополосной радиосвязи. – Одесса: Наука и техника, 2009. – 344 с.
4. Основы теории телекоммуникаций / Підручник / Під заг. ред. Ільченка М.Ю. — К.: ІССЗІ НТУУ «КПІ», 2010. — 786 с.

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ НАДАННЯ ПОСЛУГ В ВІРТУАЛЬНОМУ СЕРЕДОВИЩІ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ NGN НА БАЗІ IMS

Гогу О.П., Гаттуров В.К.

Інститут телекомунікаційних систем

КПІ ім. Ігоря Сікорського, Україна

E-mail: gogusasha25@gmail.com

Investigation opportunities for the provision services in the virtual environment of NGN telecommunication networks based on IMS

This article shows the prerequisites for the use of new carrier networking technologies and, as a consequence, the introduction of the IMS concept in the mobile network, which has led to the emergence of fundamentally new services.

Ця стаття показує передумови використання нових технологій формування мереж операторів і, як наслідок, впровадження концепції IMS в мобільній мережі, що призвело до появи принципово нових послуг.

Протягом останніх декількох років телекомунікаційна індустрія спостерігала тенденцію зростання кількості конвергентних послуг та мереж фіксованого та мобільного зв'язку, що в свою чергу привело до насичення ринку телекомунікацій та зменшення доходів операторів. В свою чергу зменшення доходів операторів напряду зв'язано зі зниженням темпів росту абонентської бази, так як і було сказано вище, ринок послуг переходить в стан насичення. Конвергенція фіксованих і мобільних технологій представляє інтеграцію технологій та послуг дротового та бездротового зв'язку для створення єдиного телекомунікаційного мережевого середовища. Така ідея обіцяє подолати деякі фізичні бар'єри, які зараз заважають провайдерам телекомунікаційних послуг досягти максимуму своїх потенційних клієнтів. Концепція IMS обіцяє зручне для оператора середовище для пакетних дзвінків та послуг у режимі реального часу, які не тільки дозволять зберегти традиційний контроль оператора над сигналізацією користувача та оплатою на основі використання, але й принесуть новий дохід з легким розгортанням широко спектру послуг користувачу. [3] Крім того, IMS архітектура проектувалася як незалежна від технології мережі доступу, що дозволяє отримувати доступ до IMS послуг з будь-якого терміналу по будь-якої зручної технології доступу (W-CDMA, GSM, LTE, LTE Advanced) [1, 2].

Мережа будь-якого оператора зв'язку складається з безлічі різноманітних спеціалізованих апаратних пристроїв, причому, ця різноманітність розширюється день у день. Запуск будь-якого нового мережевого сервісу передбачає додавання все нових наборів пристроїв, що

вимагають місця в апаратних кімнатах, нових джерел живлення, що в свою чергу призводить до збільшення затрат на підтримку мережі. Крім того, апаратні мережеві пристрої все швидше застарівають, не так фізично, скільки «морально», що вимагає все більш частих повторень циклу «закупівля - проектування - інтеграція - розгортання», причому на витратах оператора даний цикл ніяк не може залишати позитивний відбиток.

Стало ясно, що екстенсивний шлях розвитку операторських мереж на базі спеціалізованого обладнання є тупиковим. Потрібні нові підходи до розвитку бізнесу операторів і сервіс-провайдерів. Одним з таких підходів є віртуалізація мережевих функцій NFV, пов'язана з концепцією програмно-конфігурованих мереж SDN. Такий підхід може в значній мірі вирішити проблеми розгортання мережі та внесення в неї нових послуг.

Програмно-конфігуруєма мережа SDN (Software Defined Network) - це архітектурний «каркас» для створення «мереж всередині мережі» із заздалегідь визначеними параметрами і конфігурацією. Таким чином, мережа стає «програмованою», створюваною з явних ресурсів під конкретні програми і більш відкритою. SDN дозволяє автоматичне конфігурування мереж під певні програми, або набір додатків. Іншими словами сервер управління SDN автоматично конфігурує мережеві ресурси відповідно до запитів додатків.. Основна властивість архітектури SDN - відділення (абстрагування) площини пересилання пакетів (data plane) від площини управління (control plane) за допомогою стандартних протоколів між ними.

Таким чином, SDN - не черговий протокол для поліпшення роботи мережі, а нова архітектура мережі з абстрагуванням рівня управління. SDN також не є якимось новим видом мережі, який вимагає заміни обладнання або кардинальних реконструкцій. Навпаки, SDN використовує існуюче обладнання, хоча і привносить інші принципи його роботи та організації управління мережею.

Віртуалізація мережевих функцій NFV (Network Functions Virtualization) - технологія віртуалізації фізичних мережевих елементів телекомунікаційної мережі, коли мережеві функції виконуються програмними модулями, що працюють на стандартних серверах (найчастіше x86) і віртуальних машинах (VM) в них. Ці програмні модулі можуть взаємодіяти між собою для надання послуг зв'язку, чим раніше займалися апаратні платформи. Основною особливістю NFV є можливість так званої «Оркестрації послуг», тобто виділення віртуальних ресурсів тих чи інших послуг за запитом. При цьому досягається найбільш оптимальне використання ресурсів устаткування: серверів, зберігання і мережі. Для цього в архітектурі NFV передбачений компонент адміністрування і оркестрації MANO (Management and Orchestration), який є найважливішою частиною концепції NFV.

Загалом SDN та NFV не залежать один від одного, хоча NFV може в значній мірі доповнювати SDN. Архітектуру SDN / NFV зображено на рис. 1.

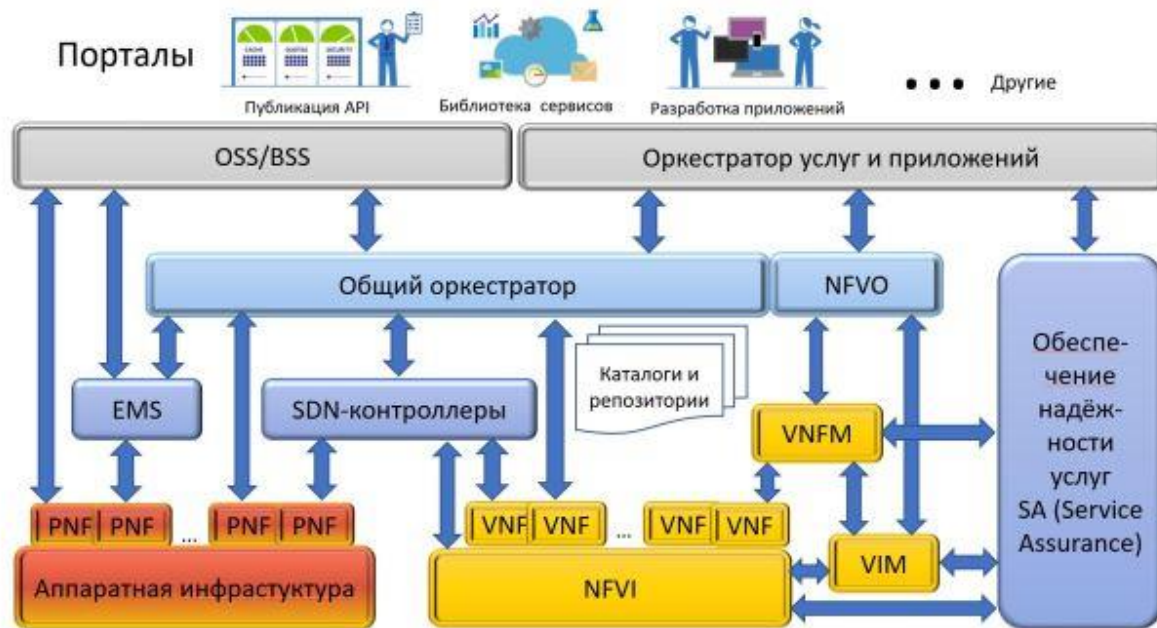


Рис.1. Архитектура SDN та NFV.

Як SDN, так і NFV, використовують хмарні та Інтернет-технології для реконструкції мереж операторів зв'язку. SDN дозволяє конфігурувати площину передачі даних програмним шляхом. NFV дозволяє задавати ролі віртуальних мережевих пристроїв також програмним шляхом. В майбутньому, всі мережеві елементи будуть розгортатися в спільно використовуваній хмарній архітектурі дата-центрів. Мережеві сценарії будуть в ній зберігатися і розвиватися відповідно до вимог додатків верхнього рівня. Це дає можливість швидко впроваджувати і розгортати нові телекомунікаційні додатки і бізнеси.

Повертаючись до мережі IMS можна сказати, що IMS це, свого роду, предтеча архітектури NFV, незважаючи на те що їх архітектури, насправді, сильно розрізняються. В архітектурі IMS вперше був реалізований принцип поділу площин даних (User Plane) і управління сесіями (Control Plane), а також рівня додатків (Application). Різниця в тому, що в NFV функції реалізуються в програмному вигляді на стандартному серверному обладнанні в дата-центрах, а IMS - на спеціалізованому телеком-обладнанні. Хоча це теж сервери, на яких працюють програми IMS, але це, все ж таки, спеціалізоване обладнання.

Література

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. Руководство по SDN и NFV/[Электронный ресурс] – режим доступа: <https://shalaginov.com/2018/01/17/%d1%80%d1%83%d0%ba%d0%be%d0%b2%d0%be%d0%b4%d1%81%d1%82%d0%b2%d0%be-%d0%bf%d0%be-sdn-nfv-2/>
4. IMS in the Next Generation Network TATIANA KOVACIKOVA, PAVOL SEGEC, MILAN KUBINA, Department of InfoCom Networks University of Zilina Univerzita .

ОЦІНКА ІНФОРМАЦІЙНОЇ ЕФЕКТИВНОСТІ СТРАТЕГІЙ ПЕРЕДАЧІ ІНФОРМАЦІЇ В МУЛЬТИСЕРВІСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Мошинська А.В.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: avmoshinskaya@gmail.com

Estimation of information efficiency of information transmission strategies in multiservice telecommunication systems

The modified technique of telecommunication technologies efficiency estimation is offered, which complements the known estimation technique for efficiency of information transmission systems, proposed by prof. Zyuko A., without changing its physical essence.

Аналіз існуючих підходів до оцінки ефективності цифрових мереж зв'язку та інформаційно-обчислювальних систем показує їх обмеженість з обліку можливостей зберігання інформації в системі, по знаходженню ступеня близькості до граничних характеристикам передачі інформації і щодо визначення оптимальних умов функціонування мережі.

В загальному випадку результат роботи системи зв'язку визначається кількістю і якістю інформації, що передається. Кількість оцінюється швидкістю передачі інформації по каналу, а якість - величиною помилки. Згідно теореми К. Шеннона, помилка при відповідному виборі методу передачі (модуляції/кодування) може бути досить малою [3].

У той же час, швидкість передачі не може бути вище деякого інформаційного ресурсу, званої пропускнуою здатністю каналу. В роботі А.Г. Зюко було запропоновано вважати одним з показників ефективності системи величину середньої швидкості, при якій забезпечується задана достовірність передачі інформації [1].

Сучасні мультисервісні телекомунікаційні системи є складними технологічними комплексами, для функціонування яких потрібні значні просторові, частотні та енергетичні ресурси. В свою чергу, ефективність використання ресурсів безпосередньо пов'язана з властивостями сигналів – переносників інформації. Властивості сигналів визначають достовірність, а значить і надійність передавання інформації в межах фізичних ресурсів, наданих мультисервісній системі. Тому оцінка на фізичному рівні ефективності мультисервісної телекомунікаційної системи та систем зв'язку як транспортної складової мультисервісної системи в рамках запропонованого матеріалу є частиною загальносистемних досліджень інформаційно-телекомунікаційних систем.

Запропонована модифікована методика оцінки ефективності телекомунікаційних технологій, яка доповнює відому методику оцінки ефективності систем передавання інформації, запропоновану проф. Зюко А.Г., не змінюючи її фізичної сутності, наступними новими можливостями:

- введення шкали узагальненої ефективності η для визначення її числових значень у діапазоні $0 < \eta \leq 1$;
- коректне відображення показників ефективності $\{\eta; \beta; \gamma\}$ на уніфікованій

шкалі для дискретних та неперервних систем передачі в області, обмеженій межею Шеннона;

- доступність комплексної оцінки інформаційної ефективності різних систем на основі трьох показників інформаційної ефективності: енергетичної β , частотної γ та узагальненої η , які роблять таку оцінку більш об'єктивною.

- розширення діапазону параметрів, які відображаються при зміні вимог до достовірності P при оцінці інформаційної ефективності різних систем передавання інформації;

- уточнення послідовності оцінки ефективності телекомунікаційних технологій з окремими видами модуляції (QAM та PSK-M).

Співвідношення для узагальненої інформаційної ефективності дорівнює:

$$\eta = \frac{R}{C} = \frac{\frac{1}{2}(\log M + P \log \frac{1}{M-1} + (1-P) \log(1-P))}{\log(1+h^2)} \quad (1)$$

де η – інформаційна ефективність; β , γ – коефіцієнти енергетичної та частотної ефективності; R – продуктивність мультисервісної системи; C – пропускна здатність каналу мультисервісної системи; P – імовірність помилки символу; h^2 – енергетичний потенціал лінії зв'язку.[2]

На рис. 1. представлено порівняння безпроводових та проводових технологій на основі показника інформаційної ефективності. Для порівняння був обраний певний набір багатократної маніпуляції (QPSK, QAM16) який використовується в кожній з технологій. При збільшенні кратності модуляції для підтримки необхідної достовірності передачі інформації $P = 10^{-5}$ - 10^{-6} спостерігається зростання показника частотної ефективності та погіршення показника енергетичної ефективності.

Технології LAN (ADSL2+, Wi-Fi) поступаються за інформаційною ефективністю технологіям MAN (UMTS, DVB-T2).

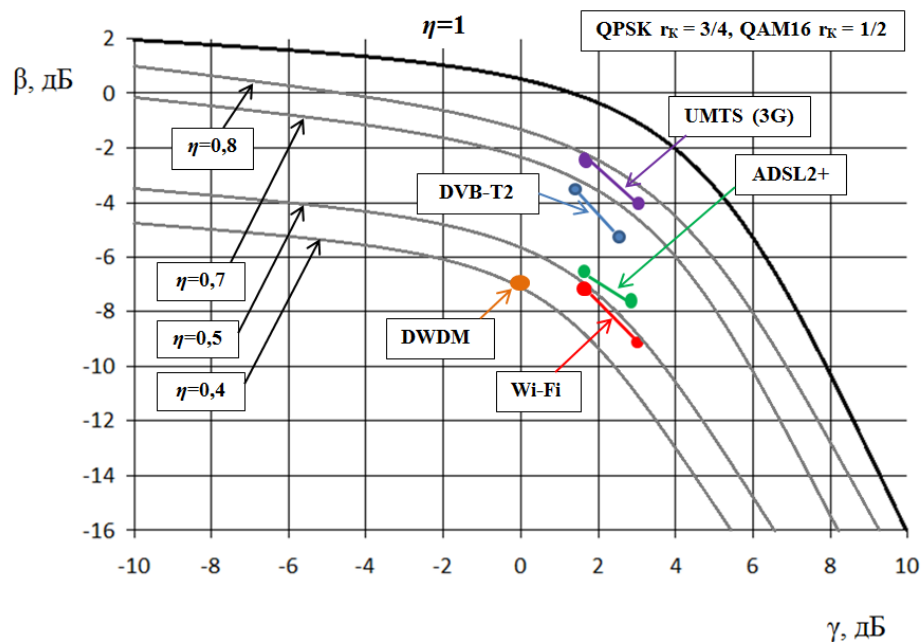


Рис. 1. Інформаційна ефективність мультисервісних телекомунікаційних систем.

Слід зазначити, що для безпроводових технологій показник енергетичної ефективності є більш чутливим, ніж для проводових. Звертаючись до технології

DWDM, можна бачити, що показники частотної та енергетичної ефективності істотно відрізняються від інших технологій в силу специфічного середовища передачі і шумових обставин в оптоволокні, а також за рахунок використання бінарних сигналів.

На рис. 2. представлені результати дослідження інформаційної ефективності для технології DVB-T2. Синьою лінією позначено зміну показників ефективності при використанні різних режимів багатократної модуляції (QPSK, QAM16, QAM64, QAM256). Швидкість кодування для даної залежності становить $r_k = 1/2$. Червоною лінією зазначено зміну показників ефективності при такому ж наборі модуляцій але швидкість кодування в цьому випадку становить $r_k = 5/6$. Для обох залежностей вимоги до достовірності складають $P=10^{-6}$.

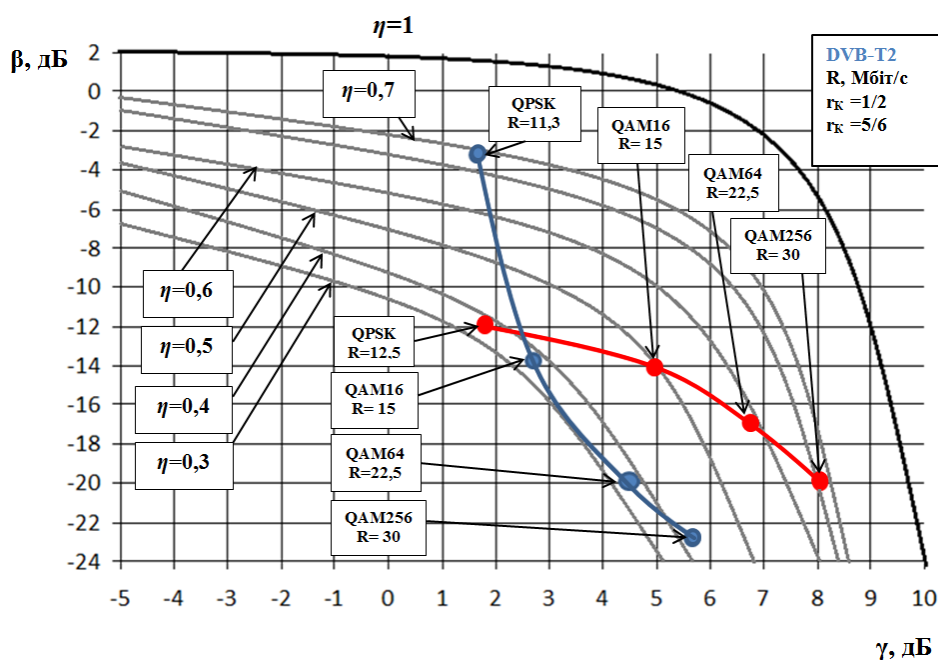


Рис. 2. Інформаційна ефективність DVB-T2.

Таким чином, червона залежність демонструє, що для досягнення достовірності $P=10^{-6}$ при швидкості кодування $r_k = 5/6$, тобто послабити вимоги до кодування в порівнянні з $r_k = 1/2$, можливо тільки у випадку збільшення відношення сигнал/шум. Це призводить до зміщення кривої вниз по шкалі енергетичної ефективності β . Одночасно, різниця між смугою частот та продуктивністю при $r_k = 5/6$ менша ніж при $r_k = 1/2$. Це призводить до зміщення кривої вправо по шкалі частотної ефективності.

Література

1. Зюко А. Г. Эффективность систем передачи сообщений / А. Г. Зюко // Электросвязь. – 1977. – № 6. – С. 17–19.
2. Уривський Л. О. Модифікована методика оцінки ефективності систем передачі інформації / Л. О. Уривський, А. В. Мошинська, К. А. Прокопенко // Наукові вісті НТУУ «КПІ». – 2010. – № 6. – С. 24–29.
3. Shannon C. A Mathematical theory of communication / C. Shannon // Bell System Technical Journal. – 1948. – Vol. 27, July and October. – P. 379–423 and 623–656.

ОРГАНІЗАЦІЯ ШИРОКОСМУГОВОГО ДОСТУПУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ PON

Григоренко О.Г., Вістунов В.Д.

Інститут телекомунікаційних систем КІП ім. Ігоря Сікорського, Україна

E-mail: olenagri@ukr.net

Implementation of broadband access using PON technology

The purpose and variants of the xPON family of technologies that provide effective broadband access while increasing customer requirements for bandwidth are analyzed.

Проаналізовані призначення та варіанти технологій сімейства xPON, що забезпечують ефективне надання широкосмугового доступу при зростаючих вимогах клієнтів до пропускної здатності.

У зв'язку зі зростанням обсягів трафіку даних, що пов'язані з появою нових технологій Інтернету речей, Big Data, штучного інтелекту тощо, а також великою кількістю нових послуг та додатків, вимоги до смуги пропускання інтернет-з'єднань будуть постійно збільшуватись, тому питання організації широкосмугового доступу і надалі залишатиметься актуальним.

Серед технологій широкосмугового доступу можна виділити проводові та безпроводові. Проводові технології в якості основних переваг використовують захищене середовище передавання, яке менш вразливе до зовнішніх завад. Окрім цього, структури даних у проводових технологіях мають менші за розміром службові заголовки з вище названих причин.

На сьогоднішній день серед проводових технологій, які використовують мідний кабель, можна виділити ADSL2+, VDSL1, VDSL2. Швидкості передачі даних в цих технологіях обмежені і залежать від відстані до абонента, і навряд чи зможуть задовольняти попит на зростаючу смугу пропускання в майбутньому. Тому перспективними виглядають технології широкосмугового доступу по оптичному волокну – технології пасивних оптичних мереж (xPON - Passive optical network) [1].

Розподільна мережа доступу PON заснована на деревовидній волоконно-кабельній архітектурі з пасивними оптичними розгалужувачами на вузлах, представляє економічний спосіб забезпечити широкосмугову передачу інформації [3]. При цьому архітектура PON володіє необхідною ефективністю нарощування вузлів мережі і пропускної здатності в залежності від наявних і майбутніх потреб абонентів.

PON використовує всього один модуль з передавачем і приймачем в OLT (Optical line terminal) для передачі інформації багатьом клієнтським пристроям ONT (Optical network terminal) або ONU (Optical network unit) і прийому інформації від них.

Число клієнтських пристроїв, підключених до одного OLT, залежить від бюджету потужності і максимальної швидкості апаратури OLT. Для передачі прямого потоку від OLT до ONT використовується оптичний сигнал з

довжиною хвилі 1490 нм. Відповідно, зворотний потік передається на довжині хвилі 1310 нм. Для передачі сигналу телебачення використовується довжина хвилі 1550 нм. В OLT і ONT вбудовані мультиплексори WDM, що розділяють вихідні і вхідні потоки. На рисунку 1 показаний приклад побудови мережі GPON.

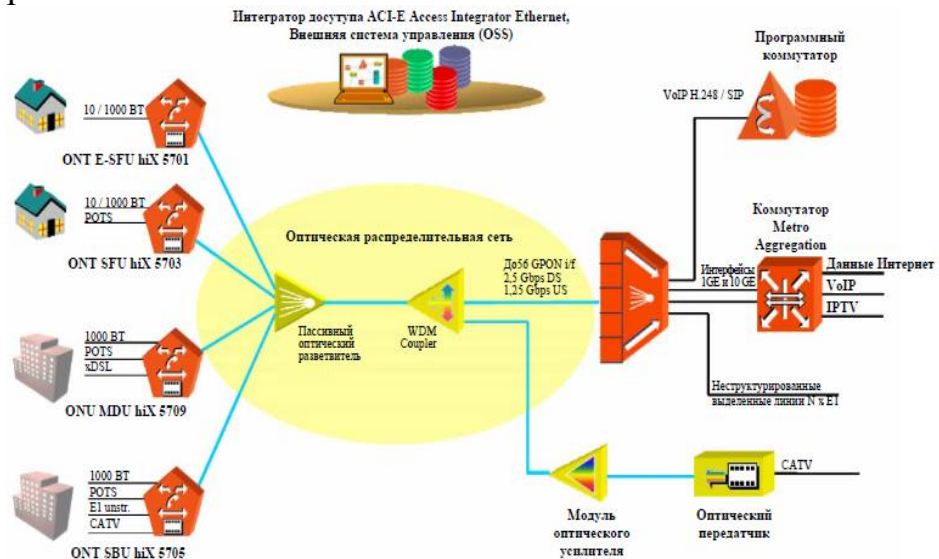


Рис.1. Приклад побудови мережі GPON.

Прямий потік розсилається всім клієнтам, але кожен ONT за своєю MAC-адресою виділяє з загального сигналу призначену тільки йому частину інформації. Зворотний потік формується на основі множинного доступу з часовим поділом (TDMA - time division multiple access), тобто для сигналу кожного ONT встановлюється свій часовий інтервал для передачі даних. При цьому враховується поправка на затримку сигналу, пов'язану з відстанню між ONT та OLT.

На сьогоднішній день актуальними технологіями сімейства xPON є GERON, GPON, XGPON, перспективною можна вважати NG-PON2.

GERON [2] використовує в якості транспортного протоколу технологію Ethernet. Низхідний потік передається зі швидкістю 1 Гбіт/с на довжині хвилі 1550 або 1490 нм, висхідний - зі швидкістю 1 Гбіт/с на довжині хвилі 1310 нм.

GPON (Gigabit PON) використовує в якості транспортного протоколу технологію SDH з протоколом формування пакетів GFP (generic framing protocol). Швидкість передавання низхідного / висхідного потоків наступна: 1244,16 Мбіт/с / 155,52 Мбіт/с; 1244,16 Мбіт/с / 622,08 Мбіт/с; 1244,16 Мбіт/с / 1244,16 Мбіт/с; 2488,32 Мбіт/с / 155,52 Мбіт/с; 2488,32 Мбіт/с / 622,08 Мбіт/с; 2488,32 Мбіт/с / 1244,16 Мбіт/с; 2488,32 Мбіт/с / 2488,32 Мбіт/с [4]. Передача інформації для висхідного потоку здійснюється в смузі 1260-1360 нм, а низхідного в смузі 1480-1580 нм.

Технологія XGPON (10GPON – 10 Гігабіт/с PON) є подальшим розвитком технології GPON і є сумісною з GPON та GERON. Низхідний потік передається в діапазоні 1260-1280 нм і висхідний – 1575-1581 нм з відстанню передачі не менше 20 км та сплітерами з кратністю ділення до 1:64. Існує два варіанти XGPON, що відрізняються швидкостями потоків:

XGPON1: 10 Гбіт/с / 2,5 Гбіт/с та XGPON2: 10 Гбіт/с / 10 Гбіт/с [5].

Технологія NG-PON2 (40GPON – 40 Гігабіт/с PON) є подальшим розвитком технології GPON і є сумісною з GPON та GPON. Системи NG-PON2 мають два варіанти. Перший, з використанням принципу одночасного мультиплексування з часовим та частотним розділенням (TWDM - Time and Wavelength Division Multiplexing), коли 4 або 8 довжин хвиль поєднують потоки від кількох xPON. Другий варіант, з використанням принципу розділення за довжиною хвилі точка-точка (PtP WDM - Point-to-Point WDM), коли на один мережний блок подається одна або кілька довжин хвиль в кожному напрямку. Відстань передачі не менше 40 км, а при певних умовах 60 км і до 100 км. Швидкості кожного TWDM каналу можуть бути такі: 10 Гбіт/с / 10 Гбіт/с; 10 Гбіт/с / 2,5 Гбіт/с; 2,5 Гбіт/с / 2,5 Гбіт/с. Кратність ділення сплітера до 1:256 [6].

У таблиці 1 наведені можливі сервіси, які можуть бути забезпечені за допомогою PON.

Таблиця 1.

Дані	- високошвидкісний Інтернет; - дані корпоративних користувачів; - приватні лінії; - Frame Relay; - з'єднання АТМ; - інтерактивні ігри; - системи безпеки і моніторингу
POTS	- одна або декілька телефонних ліній
Відео	- цифрове і аналогове ширококомове відео - телебачення високої чіткості (HDTV) - відео-на-вимогу (VoD) - інтерактивне TV / платне TV

Таким чином, проаналізувавши призначення та варіанти технологій сімейства xPON, можна зробити висновок, що технології GPON, GPON, XGPON, що використовуються українськими операторами, задовольняють сучасним вимогам до смуги пропускання. В перспективі ці технології можна буде модернізувати до сумісної технології NG-PON2.

Література

1. ITU-T. G.983.1. Оптичні системи широкосмугового доступу, що базуються на пасивній оптичній мережі (PON).
2. Kramer Glen. Ethernet Passive Optical Network (EPON)/ [Електронний ресурс] – Режим доступу: <https://www.litmir.me/a/?id=123397>
3. Гаврилов О.В. Особенности внедрения инновационной технологии Passive Optical Network (PON)/ [Електронний ресурс] – Режим доступу: <https://sibac.info/studconf/econom/xxvii/40332>
4. ITU-T. G.984.1. Gigabit-capable passive optical networks (GPON): General characteristics.
5. ITU-T. G.987.1. 10-Gigabit-capable passive optical networks (XG-PON): General requirements
6. ITU-T. G.989.1. 40-Gigabit-capable passive optical networks (NG-PON2): General requirements.

ОСОБЛИВОСТІ ОПТИЧНИХ МЕРЕЖ ДЛЯ ЗАБЕЗПЕЧЕННЯ ВИМОГ ТЕХНОЛОГІЇ 5G

Григоренко О.Г., Кочева Н.С.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: olenagri@ukr.net

Features of optical networks to provide requirements of 5G technology

Some basic requirements for fifth generation mobile networks are given. Features of optical network design and their characteristics that will provide the requirements of 5G technology are defined.

Наведені основні вимоги до мереж мобільного зв'язку п'ятого покоління. Зазначені особливості побудови та характеристики оптичних мереж, що забезпечать вимоги технології 5G.

Оптичні мережі підтримують широкий спектр послуг зв'язку, включаючи послуги «оптичне волокно до дому» (FTTH), послуги підприємств та мобільні послуги. З впровадженням послуг мобільного зв'язку 5-го покоління особливості побудови та характеристики оптичної мережі змінюються, тому є актуальним визначити ці особливості.

Очікується, що безпроводова технологія п'ятого покоління (5G) буде запуснена в глобальному масштабі в поточному 2020 році [1]. Оптична мережа, що забезпечуватиме технологію 5G, повинна відповідати трьом основним характеристикам, без яких не можливе повноцінне функціонування, а саме:

- збільшена пропускна здатність оптичного волокна;
- масові оптичні крос-з'єднання;
- інтелектуальна експлуатація та обслуговування мережі.

При забезпеченні вище зазначених характеристик мережа буде мати такі основні функції:

- розширений широкосмуговий мобільний зв'язок;
- масовий зв'язок машинного типу;
- наднадійний зв'язок з малою затримкою.

Ці три основні функції в сукупності підтримують розширений діапазон послуг і є сумісними з новими сервісами, які з'являться в епоху 5G. Також це забезпечить передачу зростаючого трафіку мереж інтернету речей.

Щоб задовольнити вимоги розширеного широкосмугового мобільного зв'язку в 5G, оптичні мережі повинні забезпечувати більшу пропускну здатність і бути економічно ефективними [2].

За період 2013-2019 рр пропускна здатність оптичного волокна зросла з 8 Тбіт/с до 32 Тбіт/с [1]. У 2013 р цифрове когерентне детектування з корекцією помилок SD-FEC (soft-decision forward-error correction) дозволило передавати канали зі швидкістю 100 Гбіт/с при квадратурній фазовій маніпуляції з розділенням за поляризацією оптичного сигналу PDM-QPSK (Polarization-division multiplexing - quadrature-phase-shift keying) на відстані

більше 4000 км.

Підсилювачі EDFA, що використовуються в оптичних мережах, забезпечують в С-діапазоні (1530-1565 нм, тобто смуга підсилення 4 ТГц) передачу по одному оптичному волокну вісімдесяти оптичних каналів зі швидкістю 100 Гбіт/с з кроком між каналами в 50 ГГц, що призводить до пропускної спроможності кожного волокна 8 Тбіт/с, на сьогодні – 32 Тбіт/с. Таким чином, спектральна ефективність системи WDM (Wavelength division multiplexing) становила 2 біт/с/Гц, яка на 2019 рік збільшилася до 5,3. Оптикоелектронні пристрої, що для модуляції/демодуляції використовують швидкості 32 Гбод, дозволяють забезпечувати швидкість даних 128 Гбіт/с при PDM-QPSK та швидкість 100 Гбіт/с після видалення службових даних для FEC. Квадратурні амплітудні модуляції (QAM) більш високого рівня, такі як PDM-64QAM, були введені для подальшого збільшення швидкостей, на 2019 рік швидкість оптикоелектронних пристроїв 64 Гбод. Цифрова обробка оптичного сигналу ґрунтувалася на 40-нм CMOS-технології, на сьогодні - 7-нм CMOS-технологія [1].

В майбутньому з використанням як розширеної С-смуги, так і розширеної L-смуги, смуга підсилення EDFA може бути збільшена до 10 ТГц. З досягненнями в технологіях оптикоелектронних пристроїв швидкість модуляції може перевищувати 100 Гбод. Більш досконалі алгоритми цифрової обробки оптичного сигналу включають імовірнісне формування сузір'я (PCS -Probabilistic constellation shaping) для QAM більш високого рівня, компенсацію нелінійності і спільну обробку складових суперканалу, які можуть бути реалізовані з використанням 5-нм CMOS-технології. При досягненні цих характеристик у 2022 році в системах передачі даних відбудеться подальше подвоєння пропускної здатності оптичних волокон до 64 Тбіт/с [1].

При використанні 5G неприпустимі довгі затримки в мережі, так як технології та додатки є чутливими до затримок і сильно залежать від швидкості передачі даних. Тому необхідно транспортувати канали систем WDM з малою затримкою, максимально використовувати оптичні крос-з'єднання для перемикавання оптичних каналів різних довжин хвиль, що забезпечить прямі з'єднання на оптичному рівні через різні вузли 5G-орієнтованих оптичних мереж.

Масові оптичні крос-з'єднання необхідні для забезпечення повної можливості перемикавання для всіх каналів WDM у всіх волокнах, підключених до оптичного вузла. Це можна забезпечити використанням багатоступеневих реконфігурованих вузлів введення/виведення оптичних каналів (MD-ROADM -multi-degree reconfigurable optical add/drop multiplexer) і компонентів оптичної крос-комутації OXC (optical cross connect). Такі вузли будуються за допомогою комутаторів, що перемикаються за довжиною хвилі (WSS - wavelength selective switch) та WXC (wavelength selective cross connect).

Рисунок 1 ілюструє вузол ROADM/OXC, що підтримує додавання/видалення будь-якої довжини хвилі з/в будь-якого напрямку.

Підсистема ROADM/OXC може стати більш компактною завдяки використанню вбудованого $N \times N$ OXC на рівні довжини хвилі для перемикання на стороні лінії і інтегрованого $N \times M$ WSS для локальних з'єднань введення/виведення і з'єднань без волокон. Нові WSS введення-виведення забезпечують знижені втрати і енергоспоживання [3].

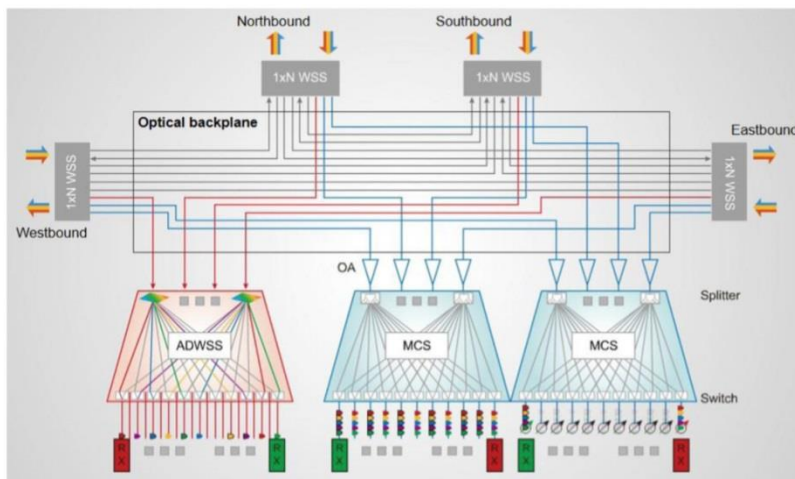


Рис. 1. Приклад вузла ROADM/OXC [1].

Максимально спростити та сконфігурувати правильність роботи мережі 5G має система інтелектуальної експлуатації та обслуговування мережі, яка надає можливості швидкого планування мережі та надійного обслуговування. На етапі експлуатації можливий прогноз трафіку, усунення несправностей і попередження про помилки. На етапі оптимізації адаптивне управління ресурсами і поділ мережі на рівні забезпечують, щоб послуга підтримувалася адекватно та зі збереженням ресурсів [4]. З впровадженням штучного інтелекту в мережевому хмарному середовищі стало можливим прогнозувати збої в оптичних мережах і майбутні вимоги до мережевих ресурсів, підвищуючи таким чином ефективність експлуатації та обслуговування.

Таким чином, для підтримки технології 5G оптичні мережі повинні забезпечувати збільшену пропускну здатність оптичного волокна; масові оптичні крос-з'єднання на базі вузла ROADM/OXC, що підтримує додавання/видалення будь-якої довжини хвилі з/в будь-якого напрямку; інтелектуальну експлуатацію та обслуговування мережі, які надають можливості надійного та адаптивного управління ресурсами.

Література

1. LIU Xiang. Evolution of Fiber-Optic Transmission and Networking toward the 5G Era/ LIU Xiang// iScience. – 2019. - Dec 22. – P.489-506. [Електронний ресурс] – Режим доступу: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6920305/>
2. Григоренко О.Г. Особливості реалізації ефективних оптичних транспортних мереж; Вісник НТУУ «КПІ», серія «Радіотехніка. Радіоапаратобудування», №73, 2018. – с.28-32.
3. COLBOURNE, Paul D., et al. Contentionless twin 8x24 WSS with low insertion loss// Optical Fiber Communication Conference. Optical Society of America. - 2018. - Th4A.
4. Vilalta R., López-de-Lerma A.M., Muñoz R., Martínez R., Casellas R. Optical Networks Virtualization and Slicing in the 5G era/ Optical Fiber Communication Conference, San Diego, USA. - 2018. - M2A.4,

РЕКОМЕНДАЦІЇ ЩОДО ПОКРАЩЕННЯ БЕЗПЕКИ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Григоренко О.Г., Полікарпова Ю.Г.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: olenagri@ukr.net, july.polik@gmail.com

Recommendations for improving the security of telecommunications networks

The main threats related to the telecommunications infrastructure are described. Recommendations for improving the security of telecommunications networks are defined.

Описані основні загрози, пов'язані з телекомунікаційною інфраструктурою. Зазначені рекомендації щодо покращення безпеки телекомунікаційних мереж.

Загрози для безпеки телекомунікаційних мереж є підставою для занепокоєння міжнародних організацій протягом останніх десятиліть. Телекомунікаційна інфраструктура, яка забезпечує необхідну основу для обміну інформацією є особливо вразливою для різних форм нападів. Деякі з цих нападів можуть призвести до відмови в обслуговуванні, втрати цілісності та конфіденційності даних та мережевих служб. Одним із контрзаходів є конфіденційність за замовчуванням, метою якої є оновлення системи при щойно виявлених загрозах.

Загрози, пов'язані з телекомунікаційною інфраструктурою, можуть здійснюватися зловмисниками з метою створення повної відмови зв'язку або отримання незаконного прибутку. Серед таких основних загроз можуть бути виділені [1,2,4]:

1. Теракти. Атаки, які здатні викликати серйозні збої мережевих сервісів, можуть бути будь-якої форми. Однією з форм є атаки в результаті військових конфліктів, що призводять до фізичного руйнування телекомунікаційного обладнання і здійснюються з боку терористів.

2. Технологічні загрози. Є наслідком самих технологій і в основному пов'язані зі споживачами телекомунікаційних послуг. У деяких випадках загроза або напад може привести до великих фінансових втрат. Прикладом може слугувати довготривалий виклик, коли «компанія-одноденка» під виглядом телекомунікаційної організації телефонує абонентам, здійснює переадресацію виклику та пропонує свої послуги. Далі така компанія може утримувати виклик без згоди або відома абонента, і такий виклик може залишатися дійсним протягом декількох днів, якщо у абонента не встановлений ліміт на дзвінок. У разі міжнародного виклику це може привести до серйозної фінансової втрати, адже абонентом може бути як окрема людина, так і організація.

3. Кримінальні злочини. Становлять небезпеку для телекомунікаційних підприємств та їх клієнтів. Наприклад: зрощення телекомунікаційного кабелю, тобто сплайсинг, і хакерство.

Зрощення телекомунікаційної кабельної розводки є процесом

отримання несанкціонованого доступу до телекомунікаційної мережі шляхом механічного приєднання до кабелю. Хакери отримують віддалений доступ до мережі, проникають всередину та компрометують і викрадають дані.

Конвенція про кіберзлочинність Ради Європи виділила вісім правопорушень з подальшою кримінальною відповідальністю: 1) незаконне перехоплення; 2) втручання в дані; 3) втручання в систему; 4) неправильне використання пристроїв; 5) підробка з використанням комп'ютерів; 6) шахрайство з використанням комп'ютерів; 7) правопорушення, пов'язані з дитячою порнографією; 8) правопорушення, пов'язані з порушенням авторського права і суміжних прав.

4. Загальні загрози та атаки. Учасниками є спеціальні державні структури. Це форма хактивізму, що спонсорується державою.

Рисунок 1 надає архітектуру безпеки, що показує, на яких рівнях потрібно вживати заходів для безпечного функціонування додатків і обміну, обробкою даних в мережі організації.

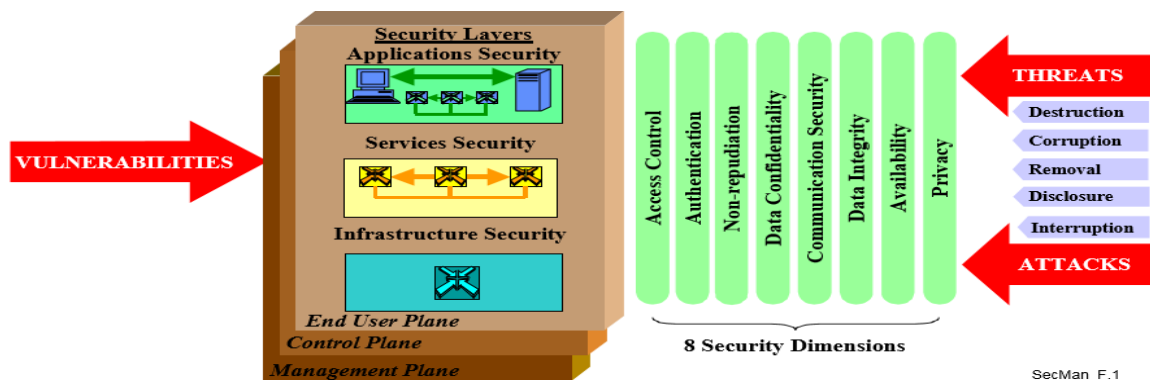


Рис.1. Елементи архітектури безпеки згідно X.805 [3].

Рекомендації щодо покращення безпеки телекомунікаційної мережі полягають в наступному:

1. Телекомунікаційна мережа безпеки.

Необхідна технологія повинна бути введена в дію для збереження телекомунікаційної інфраструктури і ресурсів. У тих регіонах, де є військові конфлікти з високою імовірністю терактів, телекомунікаційна інфраструктура на відкритому повітрі, радіоапаратура і енергогенеруючі комплекти, повинні бути розташовані у більш безпечних районах. Це необхідно, щоб уникнути фізичного знищення встановленого обладнання.

2. Операційна безпека (Operations Security, OPSEC).

OPSEC спрямована на запобігання витоків важливої інформації або процедур, що стосуються безпеки організації із зовнішнім світом. Наприклад, організація може обмежити той контент, який співробітники розміщують на своїх сторінках Facebook або інших соціальних засобах масової інформації.

3. Безпека за замовчуванням.

Організації або компанії повинні розробити систематичний метод профілактики або боротьби з нападом. Безпека за замовчуванням фокусується на трьох пунктах: 1) запобігання: проектування систем, які

важче зламати; 2) стійкість: системи проектування, які можуть запропонувати безпечні транзакції, навіть після того, як вони були скомпрометовані; 3) регенерація: системи проектування, які можуть автоматично відновити себе, коли порушення будуть виявлені.

4. Обмеження на чутливі зони.

Телекомунікаційний простір, обладнання, приміщення повинні бути надійно захищені і розглядатися як обмежені зони. Доступ до цих областей слід контролювати і надавати тільки уповноваженим особам. Такі методи, як установка управління електронного доступу (Electronic Access Controls, EAC), механічні комбінації замків, повинні бути використані для контролю доступу. Список осіб, які мають доступ до цих чутливих зон або приміщень, повинен бути збережений, щоб уникнути несанкціонованого доступу. Організація повинна також вести журнал контролю для цілей аудиту безпеки.

5. Реалізація інфраструктури безпеки [2].

Важливі політики, прийняті організацією, повинні підтримуватися інфраструктурою безпеки мережі, яка включає в себе кілька рівнів безпеки. Ця стратегія говорить про те, що жоден із рівнів безпеки не повинен відкрити мережу для атак. Деякі із заходів безпеки, які можуть бути розгорнуті на різних рівнях: 1) захищена кабельна інфраструктура; 2) фізичні механізми контролю доступу, такі як смарт-картки і біометричні зчитувачі; 3) брандмауери на периметрі мережі для публічно доступних систем; 4) хости і мережеві системи виявлення вторгнень/захисту; 5) управління зловмисними кодами за допомогою антивірусів, антишпигунських технологій; 6) безпечні методи розробки додатків; 7) проведення перевірок безпеки телекомунікаційного обладнання, території, допустимих мережевих компонентів і додатків; 8) шифрування і маскування даних; 9) розуміння безпеки.

Таким чином, телекомунікаційні мережі є великою мішенню для кіберзлочинців, тому усвідомлення сучасних загроз та створення системи заходів безпеки допоможуть організаціям зберегти конфіденційність своїх даних та забезпечити безпечне функціонування мережевої інфраструктури. Запропоновані заходи значно покращать безпеку телекомунікаційної мережі.

Література

1. Григоренко О.Г., Пчелінцев І.С. Заходи для захисту від атак для забезпечення кібербезпеки організацій// МНТК "Перспективи телекомунікацій-2019" - Київ; Дата проведення: 17.04.2019.
2. Security in Telecommunications and Information Technology/ [Електронний ресурс] – Режим доступу: <https://www.itu.int/itudoc/itu-t/85097.pdf>.
3. ITU-T. X.805 Security architecture for systems providing end-to-end communications.
4. Северина С.В. Інформаційна безпека та методи захисту інформації /С.В.Северина// Вісник Запорізького національного університету. - 2016. - № 1 (29). – С.155-161. [Електронний ресурс] – Режим доступу: [http:// www.irbis-nbuv.gov.ua > cgi-bin > irbis_nbuv > cgiirbis_64 > Vznu_](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64/Vznu_).

ПОБУДОВА ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ НА ОСНОВІ ОБЛАДНАННЯ ФІРМИ CISCO

Волік Д. В., Григоренко О.Г.

Інститут телекомунікаційних систем КІП ім. Ігоря Сікорського, Україна

E-mail: stormfall927@gmail.com, olenagri@ukr.net

Design of virtual private networks based on CISCO equipment

Theoretical base, statistics, methods for setting up and implementing virtual private networks are given. The classification and comparison of different types of virtual private networks (VPNs) are also shown.

Наведено термінологію, статистичні дані, методи налаштування віртуальних приватних мереж та їх реалізація. Зображено класифікацію, а також порівняння різних типів віртуальних приватних мереж (VPN).

Віртуальні приватні мережі (VPN) використовуються у всьому світі, щоб забезпечити зашифровані підключення до Інтернету. Це надає можливість користуватися мережею Інтернет з підвищеною конфіденційністю. Більше того, VPN може замінити справжню IP-адресу на іншу з іншого регіону, що дозволяє отримувати інформацію, доступ до якої раніше був заблокований.

Ринок VPN невинно зростає. Згідно з дослідженнями компанії Knowledge Sourcing Intelligence LLP, ринок VPN буде зростати з темпами 6,39% на рік протягом наступних п'яти років [1]. У 2018 році ринок охоплював близько 34,6 мільярда доларів, тож, враховуючи цей темп, до 2024 року його обсяг сягне понад 50 мільярдів доларів. У звіті основною причиною зростання попиту зазначаються проблеми кібербезпеки. Однак, оскільки VPN направляє дані на інший сервер перед тим, як перенести користувача на потрібну веб-сторінку, з'являються певні проблеми із продуктивністю та швидкістю, що частково стримує попит на ці послуги протягом прогнозованого періоду.

Віртуальні приватні мережі також можуть слугувати і для організації мереж без шифрування, тобто загальнодоступних. Існує низка способів реалізації VPN з використанням таких технологій, як GRE, SSL, IPsec та ін. Побудова віртуальних приватних мереж включає в себе створення тунелів, що являють собою канали, які сполучають два пристрої. Цими каналами і передаються дані. Налаштування тунелів - обов'язкова задача мережевого інженера при реалізації VPN. Тунелі поділяються на два типи [2]:

1. **Remote Access VPN** – тунель сполучає комп'ютер користувача з відповідним програмним забезпеченням та будь-який пристрій, що виконує роль сервера і реалізує підключення клієнтів. Ним може бути маршрутизатор, VPN-концентратор, Cisco ASA і т. п.

2. **Site-to-Site VPN** – передбачає постійний тунель між двома пристроями (наприклад, маршрутизаторами). Користувачі ж знаходяться у локальних мережах (LAN) і даний спосіб тунелювання не потребує

завантаження спеціалізованого програмного забезпечення.

Нижче наведено приклади використання цих технологій.

Перший тип застосовується, коли необхідно забезпечити підключення віддалених співробітників до корпоративної мережі за допомогою захищеного каналу. В даному випадку, якщо користувач має стабільне інтернет-з'єднання та завантажив відповідне програмне забезпечення, комп'ютер самостійно побудує даний тунель до маршрутизатора компанії.

Другий тип часто використовується за необхідності з'єднання віддалених мереж, наприклад, філіалів або філіалу з центральним офісом. Роботу зі створення тунелю виконує сам граничний маршрутизатор. Він будує віддалене з'єднання від маршрутизатора з локальної мережі користувача – тунель, отже, співробітник без спеціалізованого програмного забезпечення здатний працювати у локальній мережі офісу.

З точки зору мережевого інженера, більших знань та навичок потребує реалізація Site-to-Site VPN. Два способи налаштування захищеного доступу між двома офісами, а саме алгоритми, полягають у наступному [3].

Перший спосіб – *використання тунельних інтерфейсів*. Він доречний у випадку створення тунелю між двома маршрутизаторами Cisco.

Кроки реалізації:

1. Вибір параметрів шифрування для тунелю;
2. Ключі шифрування. Вони мають бути спільними на обох маршрутизаторах. Рекомендовано зробити їх довгими за 50 символів та використовувати букви різного регістру, цифри та спеціальні символи для більшої безпеки;
3. Створення віртуальних тунельних інтерфейсів для кожного офісу. Якщо їх налаштування виконано правильно, стан інтерфейсів буде показаний як "up";
4. Перевірка роботи VPN-тунелю за допомогою команди ping;
5. Налаштування маршрутизації, для того, щоб мережі мали доступ одна до одної.

Другий спосіб – *універсальний*. Він підходить, коли тунель встановлюється між маршрутизатором та Cisco ASA або іншим пристроєм, що підтримує технологію IPsec VPN, не обов'язково виробництва Cisco.

Кроки реалізації:

1. Вибір параметрів шифрування для тунелю;
 2. Ключі шифрування. Вимоги як для першого способу;
 3. Об'єкти шифрування. Зазначається трафік, що має бути зашифрований;
 4. Політика шифрування. Для кожної з мереж створюється політика crypto map, у якій надаються правила та параметри шифрування;
 5. Налаштування маршрутизації, для того, щоб мережі мали доступ одна до одної;
 6. Перевірка роботи VPN-тунелю за допомогою команди ping.
- В таблиці 1 надано порівняння двох часто використовуваних типів VPN:

Назва	Cisco GRE VPN	Традиційні IP Sec VPN
Переваги	- Забезпечує передачу широкомовного і маршрутизаційного трафіку через тунелі IPSec VPN - Підтримка протоколів відмінних від IP - підтримка QoS	- Функції захисту переданого між двома точками трафіку - підтримка QoS
Причини застосування	- При необхідності маршрутизації в мережі VPN - Реалізує функції аналогічні топології зірка DMVPN, але вимагає більш об'ємної і детальної конфігурації	- При побудові мережі з обладнання різних виробників
Сумісність обладнання	Тільки маршрутизатори Cisco	Повна, у тому числі від різних виробників
Масштабування	Тисячі пристроїв у мережі	Тисячі пристроїв у мережі
Управління та контроль	Cisco Security Manager, Cisco Router and Security Device Manager	Cisco Security Manager, Cisco Router and Security Device Manager
Топологія	Зірка, невеликі повнозв'язні мережі VPN	Зірка, невеликі повнозв'язні мережі VPN
Динамічна маршрутизація	Підтримується	Підтримується
Якість обслуговування	Підтримується	Підтримується
Широкомовний трафік	Через тунель VPN	Ні
Підтримка протоколів, відмінних від IP	Так	Ні
Резервування	Засобами протоколів маршрутизації	Можливість активізації резервного каналу

Таким чином, зі збільшенням кіберзагроз у сучасному світі впровадження віртуальних приватних мереж є і буде залишатися актуальним. Шифрування трафіку та ізолюваність VPN є основними рисами, що забезпечують конфіденційність даних в телекомунікаційних мережах.

Література

1. Aimee O'Driscoll / VPN statistics: What the numbers tell us about VPNs // UPDATED: February 25, 2020 [Електронний ресурс] – Режим доступу: <https://www.comparitech.com/vpn/vpn-statistics/>
2. Bacek / Принципы организации VPN // [Електронний ресурс] – Режим доступу: <http://ciscotips.ru/vpn>
3. Nevidimkastd / VPN между двумя маршрутизаторами Cisco // Март 15, 2015 // [Електронний ресурс] – Режим доступу: <https://deltaconfig.ru/router-site-to-site-vpn/>
4. «Технориум» - интеграция / Развертывание виртуальных частных сетей VPN // Сравнение технологий построения VPN [Електронний ресурс] – Режим доступу: <http://www.technorium.ru/vpn/compare-vpn-cisco.shtml>.

ПІДХОДИ ЩОДО РОЗРОБКИ РЕКОМЕНДАЦІЙ ПО ВИБОРУ ВИДУ ЛІНІЙНОГО СИГНАЛУ В МЕРЕЖАХ ДОСТУПУ SHDSL

Носков В.І.

Інститут телекомунікаційних систем КПП ім. Ігоря Сікорського, Україна

E-mail: nvi2010@ukr.net

Approaches concerning the recommendation for choosing of the line signal type in SHDSL access networks

In access networks based on copper cable, SHDSL technology is widely used. SHDSL equipment has the possibility to choose PAM line signal with different constellation. However, in existing manual you do not find clear rules concerning the choosing of line signal depending of conditions for using the equipment. This report is devoted to finding the approaches for such recommendations.

У мережах доступу, що у якості середовища передачі використовують мідний кабель, є поширеною технологія SHDSL. Сучасне обладнання SHDSL має можливість при конфігуруванні вибирати різні варіанти лінійного сигналу виду PAM, від TC-PAM16 до TC-PAM128. Тому актуальною задачею є розробка рекомендацій щодо вибору виду модуляції. Деякі підходи до вирішення цієї задачі наведені у даній доповіді.

Одним з напрямків пошуку підходів в формулюванні рекомендацій щодо вибору лінійного сигналу може бути порівняння запасу завадостійкості (SQ) для певних відстаней та швидкостей передачі при різних видах модуляції.

Відомо, що коефіцієнт помилок (BER) є функцією від співвідношення енергії сигналу у перерахунку на 1 біт до спектральної щільності завад у точці прийому (для спрощення розрахунків будемо вважати, що діють тільки теплові шуми):

$$BER = f(h^2),$$

де: $h^2 = \frac{E}{N_0}$; $E = P_c \cdot T_c = \frac{P_c}{R}$ – енергія 1 біту сигналу у точці прийому; R – бітова швидкість передачі; P_c – потужність сигналу у точці прийому; N_0 – спектральна щільність теплових шумів.

Спектральна щільність теплових шумів відповідно до прийнятої моделі теплових шумів у системі G.SHDSL не залежить від частоти та дорівнює $N_0 = -120$ дБм/Гц, або 10^{-12} мВт/Гц.

Потужність сигналу у точці прийому визначається як:

$$P_c = \int_{F1}^{F2} (PSD_{tx}(f) / L(f)) df, \quad (1)$$

де: $PSD_{tx}(f)$ – спектральна щільність сигналу на виході передавача; $L(f)$ –

згасання сигналу у кабельній лінії; $F1 = 5$ кГц – мінімальна частота спектру лінійного сигналу ТС-РАМ; $F2 = f_{\text{sym}}/2$ – максимальна частота спектру лінійного сигналу ТС-РАМ; $f_{\text{sym}} = (R+8000)/K$ – символна швидкість модуляції; K – кількість інформаційних символів у модуляційному блоці (ТС-РАМ16 – 3; ТС-РАМ32 – 4; ТС-РАМ64 – 5; ТС-РАМ128 – 6).

Спектральна щільність сигналу на виході передавача визначається як [1,2]:

$$PSD_{tx}(f), \text{ дБм/Гц} = \frac{PSHDSL}{135} \times \frac{1}{f_{\text{sym}}} \times \left(\frac{\sin(\frac{\pi f}{f_{\text{sym}}})}{\frac{\pi f}{f_{\text{sym}}}} \right)^2 \times \frac{1}{1 + \left(\frac{f}{F2} \right)^{2 \times \text{order}}} \times \frac{f^2}{f^2 + F1^2}, \quad (2)$$

де: $PSHDSL = 7,86$ ($R < 2048$ кбіт/с) та $9,90$ ($R \geq 2048$ кбіт/с) – масштабний коефіцієнт; $\text{order} = 6$ – порядок згладжувального фільтру на виході передавача.

Згасання сигналу у кабельній лінії визначається наступним чином [3]:

$$L(f), \text{ дБ} = D \times 8,69 \times \sqrt{\frac{1}{2}(rg - lc(2\pi f)^2 + \sqrt{(r^2 + l^2(2\pi f)^2)(g^2 + c^2(2\pi f)^2)}), \quad (3)$$

де: r, g, c, l – погонні опір, провідність ізоляції, ємність та індуктивність пари кабелю, відповідно; D , км – довжина лінії.

Коефіцієнт помилок (BER) для сигналу з модуляцією РАМ може бути визначеним за приблизною формулою, яка відноситься до систем передачі з некогерентною обробкою багатопозиційних сигналів:

$$BER \approx (M - 1)e^{-\frac{h^2}{2(M-1)}}, \quad (4)$$

де: $M = 16, 32, 64, 128$ – позиційність РАМ-модуляції.

Оскільки побудова модулятора відповідає принципам сигнально-кодових конструкцій, то треба ще враховувати вираш від застосування завадостійкого кодування, що складає близько 3 дБ.

Таким чином, з одного боку збільшення позиційності модуляції РАМ зменшує втрати сигналу в кабельній лінії, а з другого боку різко погіршується завадостійкість системи передачі. Тому для певної швидкості передачі та довжини кабельної лінії може існувати оптимальне з точки зору максимальної завадостійкості значення позиційності РАМ. Також треба враховувати і вплив систем SHDSL на інші системи DSL-доступу, що працюють у тому ж самому кабелю. Перехідні завади зменшуються пропорційно звуженню спектру SHDSL, ширина якого тим менша, чим більша позиційність модуляції.

Запас завадостійкості SQ є різниця між h^2 для даної відстані та швидкості, що може бути розрахованим за формулами (1...3), та h^2 , що потребується для забезпечення заданого коефіцієнту помилок (розраховується за формулою 4).

У якості прикладу для пояснення підходів до вибору виду модуляції нижче наведені розрахунки запасу завадостійкості для кабелю ТПП Nx2x0,5, різних видів модуляції, довжин траси та для швидкостей 2 та 4 Мбіт/с (табл.1 та табл.2).

Таблиця 1. Швидкість 2 Мбіт/с.

Довжина траси, км		2	3	4	5	6
ТС-РАМ16	h^2 потр., дБ	24,5				
	h^2 розр., дБ	51,48	41,47	31,46	21,45	11,44
	SQ, дБ	26,98	16,97	6,96	-3,05	-13,06
ТС-РАМ32	h^2 потр., дБ	27,85				
	h^2 розр., дБ	53,06	43,84	34,62	25,4	16,18
	SQ, дБ	25,21	15,99	6,77	-2,45	-11,67
ТС-РАМ64	h^2 потр., дБ	31,1				
	h^2 розр., дБ	54,76	46,39	38,02	29,65	21,28
	SQ, дБ	23,66	15,29	6,92	-1,45	-9,82
ТС-РАМ128	h^2 потр., дБ	34,3				
	h^2 розр., дБ	56,22	48,58	40,94	33,3	25,66
	SQ, дБ	21,92	14,28	6,64	-1	-8,64

Таблиця 2. Швидкість 4 Мбіт/с.

Довжина траси, км		2	3	4	5	6
ТС-РАМ16	h^2 потр., дБ	24,5				
	h^2 розр., дБ	41	27,25	13,5	-0,25	-14
	SQ, дБ	16,5	2,75	-11	-24,75	-38,5
ТС-РАМ32	h^2 потр., дБ	27,85				
	h^2 розр., дБ	43,26	30,64	18,02	5,4	-7,22
	SQ, дБ	15,41	2,79	-9,83	-22,45	-35,07
ТС-РАМ64	h^2 потр., дБ	31,1				
	h^2 розр., дБ	45,88	34,57	23,26	11,95	0,64
	SQ, дБ	14,78	3,47	-7,84	-19,15	-30,46
ТС-РАМ128	h^2 потр., дБ	34,3				
	h^2 розр., дБ	48,48	38,47	28,46	18,45	8,44
	SQ, дБ	14,18	4,17	-5,84	-15,85	-25,86

У вищенаведених таблицях: h^2 потр. – потрібне значення h^2 для забезпечення коефіцієнту помилок 10^{-7} ; h^2 розр. – результат розрахунку h^2 для різних довжин траси.

З наведених таблиць можна зробити наступні висновки:

1. Для швидкості 2 Мбіт/с оптимальним з точки зору максимуму SQ є вид модуляції ТС-РАМ16.

2. Для швидкості 4 Мбіт/с та відстаней менших за 2 км оптимальним за тим же критерієм є ТС-РАМ16. При більших довжинах траси доцільніше використовувати ТС-РАМ128.

3. Даний підхід можливо використовувати для інших значень швидкостей та відстаней.

Література

- ITU-T Recommendation G.991.2, 2003.
- В.А. Балашов и др.. Технологии широкополосного доступа xDSL – М.: Эко-Трендз, 2009. 256с.: ил.
- Cable reference models for simulating metallic access networks. ETSI STC TM6.

МАКСИМАЛЬНЕ НАБЛИЖЕННЯ ШВИДКОСТЕЙ ПЕРЕДАЧІ ВОСП ХМ ДО ГРАНИЧНИХ МЕЖ

Буханець О.С., Бердников О.М.

Інститут спеціального зв'язку та захисту інформації, КПІ ім. Ігоря Сікорського, Україна

E-mail: sanya05091997@gmail.com

Maximum approximation of transmission speed of ВОСП ХМ to limit limits

Maximum throughput of ВОСП ХМ is analyzed. The graphs and diagrams of the comparison of the laser instability of the DWDM and NWDM technologies are presented.

Останні десятиліття характеризуються явно вираженим процесом інтеграції інформаційних систем та телекомунікаційних технологій, що останнім часом пов'язане з діджиталізацією суспільства, в тому числі і в Україні. Цей процес об'єктивно визначає неминучість подальшого розвитку інформаційного суспільства, що характеризується широким упровадженням додаткових мультимедійних послуг, високим зростанням обсягу інформаційного обміну у всесвітній мережі Internet, масовим впровадженням технологій високошвидкісної передачі цифрових сигналів із комутацією пакетів. Такі вимоги зажадають підвищення пропускної спроможності та гнучкості інформаційних мереж, надійності та безпеки систем зв'язку.

Реалізація цих процесів вимагає неухильного збільшення пропускної спроможності Національної телекомунікаційної мережі України (НТМУ), підвищення її гнучкості, забезпечення ефективної маршрутизації при передачі текстової та мовної інформації, рухомих і нерухомих зображень, інших мультимедійних послуг. Серед основних компонентів НТМУ, що напряду відповідають за пропускну спроможність мережі, є оптична транспортна платформа (ОТП), яка сформована телекомунікаційними транспортними системами (ТТС). Інтегральною оцінкою таких систем, як раз є пропускна спроможність, що визначається швидкістю (V , Гбіт/с) та дальністю передачі (L , км) лінійного сигналу. В якості ТТС на телекомунікаційних транспортних мережах і мережах доступу ще з кінця минулого століття використовуються волоконно-оптичні системи передачі (ВОСП) [1, 3].

За цей період з ними сталася помітна трансформація в бік збільшення швидкостей передачі сигналів в оптичних лінійних трактах (ОЛТ) систем передачі. Якщо при використанні ТТС плетіохронної цифрової ієрархії вона становила десятки і сотні мегабіт в секунду, при переході до ТТС синхронної цифрової ієрархії (СЦІ) – 10 і 40 Гбіт/с, то сьогодні швидкості передачі в ОЛТ, що використовують технологію хвильового мультиплексування (ХМ – *Wavelength Division Multiplexing / WDM*) тільки для C -діапазону довжин хвиль (найбільш використовуваний в Україні) складають терабіти в секунду [2].

Визначимо максимальне наближення до можливих швидкостей передачі ВОСП ХМ для C -діапазону (1530...1565 нм), які застосовують обробку сигналів в ОЛТ з використанням модуляції випромінювання лазера за

інтенсивністю (МІ), або бінарна амплітудна маніпуляція. Прийнемо для такого аналізу, що оптичний спектр випромінювання лазера обмежений трьома основними складовими, а нестабільність його випромінювання варіюється в межах 0,005...0,05 нм. Приклад обліку зазначених умов пояснює табл. 1.

Таблиця 1. Приклад розрахунку полоси частот модульованого оптичного сигналу.

Робоча довжина хвилі лазера (з нестабільністю): $\lambda_0 \pm \Delta\lambda/2$	1558,97 $\pm$ 0,05 нм
Межі зміни довжини хвилі лазера внаслідок нестабільності його випромінювання: $\lambda_0 - \Delta\lambda/2 \dots \lambda_0 + \Delta\lambda/2$	1558,92 ... 1559,02 нм
Межі зміни частоти лазера внаслідок нестабільності:	От 192 295 до 192 307 ГГц
Діапазон зміни частоти лазера внаслідок нестабільності:	12 ГГц
Нестабільність роботи лазера по частоті: $\pm \Delta f/2$	$\pm$ 6 ГГц
Необхідна смуга частот для передачі спектра модульованого сигналу по ОВ, з урахуванням нестабільності роботи лазера: $(f_0 + F_m + \Delta f/2) - (f_0 - F_m - \Delta f/2)$	$(192300 + 40 + 6) = 192346 -$ $(192300 - 40 - 6) = 192254$ 92 ГГц

Швидкість передачі ВОСП ХМ ($V_{СП}$), в першу чергу, залежить від кількості ($N_{ОТр}$) оптичних трактів / каналів (ОТр), що утворені системою, і максимально можливою швидкістю передачі трафіку по утворених ОТр ($V_{ОТр}$), тобто $V_{СП} = N_{ОТр} \times V_{ОТр}$. Кількість ОТр ВОСП ХМ залежить від використовуваної технології ХМ і діапазону роботи ВОСП (табл. 2). Швидкість передачі по ОТр визначається смугою частот або діапазоном довжин хвиль, що займані ОТр. Відомо, що швидкість передачі цифрового сигналу чисельно дорівнює тактовій частоті. Якщо по ОТр передавати трафік зі швидкістю передачі $V_{ОТр} = 40$ Гбіт/с, то тактова частота складає $F_m = 40$ ГГц, а з урахуванням випромінювання лазера на трьох складових f_0 , $(f_0 + F_m)$ і $(f_0 - F_m)$, мінімально необхідна смуга частот ОТр (Δf_{min}) буде не менше 80 ГГц. Якщо по ОТр передавати трафік зі швидкістю передачі $V_{ОТр} = 10$ Гбіт/с, то при тих же умовах Δf_{min} – не менше 20 ГГц. Тому, при передачі по ОТр потоків технології СЦІ, однакові швидкості передачі в ОЛТ ХМ в С-діапазоні забезпечують ВОСП DWDM і ВОСП NWDM (табл. 2).

Таблиця 2. Порівняння характеристик ВОСП ХМ С-діапазону довжин хвиль / частот.

Технології		WDM – просте ХМ	DWDM – щільне ХМ	HDWDM – високощільне ХМ	NWDM – вужькополосне ХМ
Смуга ОТр	$\Delta\lambda_{ОТр}$, нм	1,61	0,8	0,4	0,2
	$\Delta f_{ОТр}$, ГГц	200	100	50	25
$N_{ОТр}$		20	40	80	160
$V_{ОТр}$, Гбіт/с		40	40	10	10
$V_{СП}$, Тбіт/с		0,8	1,6	0,8	1,6

Залишається питання про показник переваги зазначених технологій. Таким показником можна якісно і кількісно визначити переваги між ВОСП за технологіями DWDM і NWDM спираючись на вимоги до нестабільності випромінювання лазерів оптичних передавачів, які можуть значно збільшити Δf_{min} . Якісно це означає що, чим більша нестабільність випромінювання лазерів ($\Delta\lambda/2$) допускається при передачі сигналу, тим доцільніше використовувати ту чи іншу з систем ХМ і навпаки. Отримані в результаті розрахунків залежності рис. 1 і 2 дозволяють зробити перший висновок, що по

нестабільності випромінювання лазерів ($\Delta\lambda/2$) доцільніше звернутися до ВОСП *DWDM*. У таких системах допускається робота при $\Delta\lambda/2 = \pm 0,05$ нм (рис. 1), а в ВОСП *NWDM* тільки при $\Delta\lambda/2 \approx \pm 0,02$ нм (рис. 2).

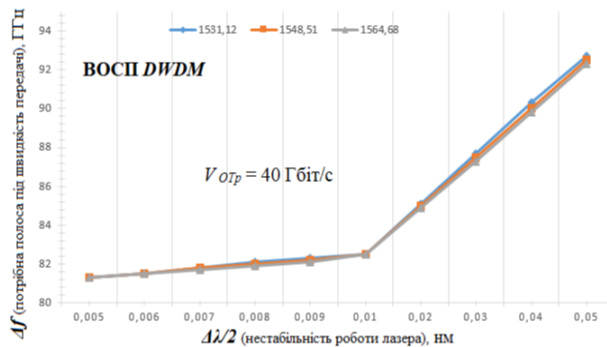


Рисунок 1.

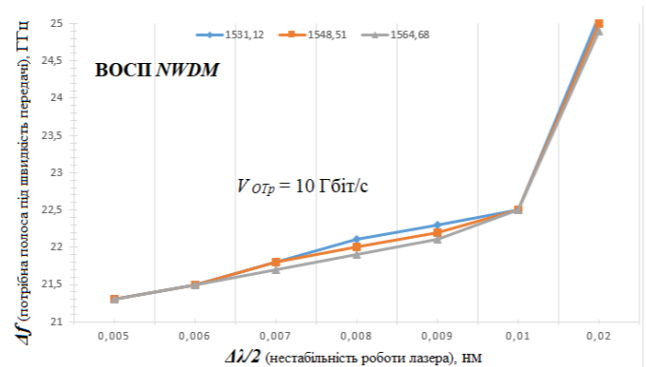


Рисунок 2.

Другим висновком є те що, критерієм кількісного порівняння ВОСП *DWDM* і *NWDM* пропонується ввести “індекс селективності”, наприклад, $\nu = \Delta f_{OTP} / \Delta f_{min}$. Такий параметр показує вираш в використанні відведеної смуги частот / довжин хвиль при передачі сигналу по ОТР з урахуванням нестабільності випромінювання лазера – $\Delta\lambda/2$. При розрахунку Δf_{min} враховувалися різні значення $\Delta\lambda/2$, а потім узагальнювалися результати за ν -індексом.

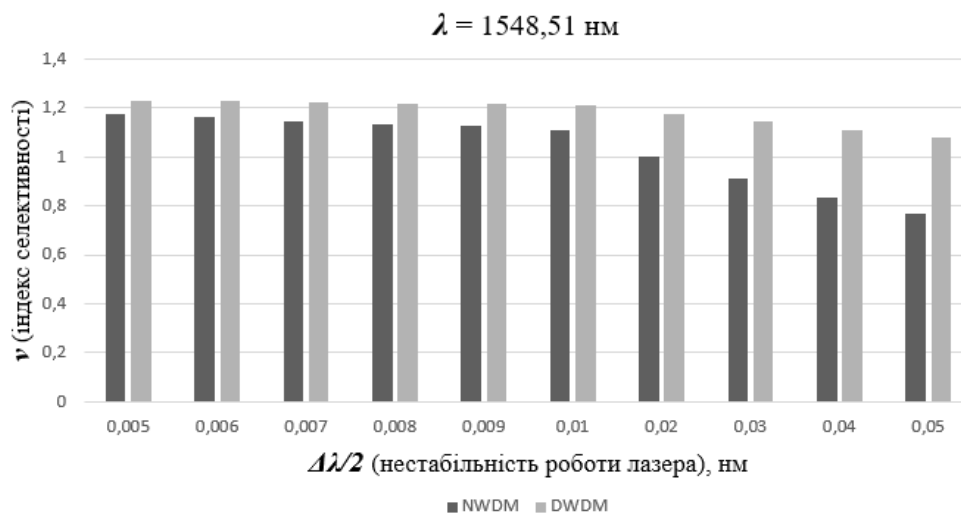


Рисунок 3.

Виграш, що отриманий, дозволяє спростити вимоги до селективних пристроїв ВОСП ХМ таких як, оптичні мультиплексори / демультиплексори, смугові фільтри, транспондери передачі і т. ін.. Доцільність застосування ВОСП *DWDM* при прийнятих умовах демонструють діаграми рис. 3, що наведені для однієї з довжин хвиль *C*-діапазону, зважаючи на повторюваність результатів на інших довжинах хвиль.

Література

1. Хмелев К.Ф. Основы фотонного транспорта. – Киев: Техніка. 2008. – 680 с.
2. Бердников О.М., Хмельов К.П. Застосування технології *WDM* на телекомунікаційних мережах / Збірник наукових праць ВІПІ НТУУ “КПІ”. – 2003. – № 3. – с. 5...11.
3. Романишин В.С., Бердников О.М. Нарощування пропускної спроможності телекомунікаційних транспортних систем. XII Міжнародна науково-технічна конференція “Проблеми телекомунікацій” ПТ-2018: Збірник матеріалів конференції. – К.: КПІ ім. Ігоря Сікорського, 2018. – С. 74...76.

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ ТЕХНОЛОГІЇ ПЕРЕДАЧІ ГОЛОСУ В МЕРЕЖІ LTE

Ветошко І.П., Носков В.І

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського

E-mail: ivanvetoshko16@gmail.com

Features of voice technology implementation on LTE networks

In this paper LTE voice technology is considered. The effectiveness and benefits of the implementation were analyzed. The concept of IMS as a support network for the organization of voice services is given.

В доповіді розглянуто технологію передачі голосу в мережі LTE. Проаналізовано ефективність та переваги її впровадження. Приведена концепція IMS, як стратегія створення опорної мережі для організації голосових сервісів.

Тема, що обговорюється в роботі є актуальною і перспективною, її дослідження дозволяє проаналізувати ефективність і переваги впровадження технології VoLTE.

У сучасному світі, коли потреби користувачів мобільного зв'язку з кожним днем зростають, операторам доводиться впроваджувати та застосовувати нові технології. Оскільки більшість людей на сьогодні вже є клієнтами того чи іншого провайдера, то постає проблема в розширенні абонентської бази. Для того, щоб залучити нових абонентів, оператори намагаються осучаснювати свою інфраструктуру, надавати відмінну якість сервісів та вводити нові види послуг. Таким чином між операторами розгортається справжня боротьба за лідерство на ринку. Голосовий зв'язок перестає бути основним джерелом доходу операторів, проте даний сервіс все ще популярний серед абонентів.

Сьогодні спостерігається стрімке збільшення обсягів споживання мобільного трафіку, що в свою чергу стимулює операторів до нарощування власних потужностей. Впровадження таких дорогих технологій як, LTE (Long-Term Evolution) та LTE Advanced дає змогу різко підвищити обсяги передачі даних, що відповідно приносить значні прибутки компаніям. Проте LTE передбачає передачу даних тільки у вигляді IP-пакетів. Тому для забезпечення функціонування голосових сервісів, пропонується концепція IMS (IP Multimedia Subsystem). На основі IMS в мережах 4G реалізується технологія передачі голоса VoLTE (Voice over Long-Term Evolution).

На мережах операторів наразі широко використовується процедура переходу з мережі четвертого покоління в 3G та 2G. Вона має назву CS FallBack (Circuit Switched FallBack). Дана процедура виконується, коли

абонент здійснює або приймає виклик. В 3G/2G архітектурі присутні 2 домени: CS Core (Circuit Switched Core) та PS Core (Packet Switched Core). Саме тому відбувається розподілення голосу та даних. Голосовий трафік проходить в мережі з комутацією каналів через CS Core, а пакетний трафік в мережі з комутацією пакетів через PS Core. При реалізації технології VoLTE весь трафік буде проходити в доменах 4G: EPC (Evolved Packet Core) та IMS. На рис. 1 зображена поетапна міграція трафіку з 3G/2G в LTE.

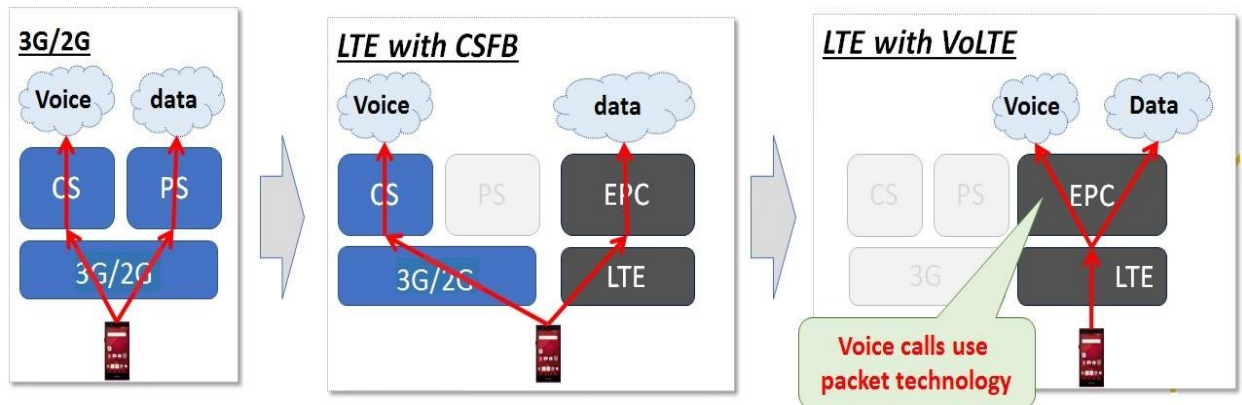


Рис. 1. Міграція трафіку з 3G/2G в LTE.

При використанні VoLTE, як основний спосіб передачі голосу в мережах четвертого покоління, оператор та абонент отримують вагомі переваги. Перш за все, це швидкість з'єднання мобільних пристроїв. Завдяки тому, що відсутній CSFB (LTE-терміналам не потрібно переходити в 3G/2G), з'єднання між ними відбувається миттєво. Це забезпечує менші витрати заряду акумулятора. А ще, оскільки LTE є пріоритетною мережею, то при вхідних і вихідних викликах, передача даних може продовжуватися без зниження швидкості.

Іншою перевагою є те, що тепер немає жорстких обмежень на полосу пропускання, це дозволяє забезпечити високу якість голосу (HD-Voice). При впровадженні ядра IMS з'являється багато можливостей для реалізації нових послуг. Прикладом можуть бути сесії відео-викликів, відео-конференцій та інші.

Недоліком мереж 4G/LTE є недостатнє покриття територій. В цьому випадку мережі попереднього покоління мають значні переваги. Оскільки, проникність невисока, це ставить під сумнів раціональність введення технології VoLTE.

Голосовий потік є чутливим до характеристик передачі (затримка, джиттер). Для забезпечення якості, передбачено підтримка QoS (Quality of Service). Стандартом LTE вибрано набір ідентифікаторів QCI (QoS Class Identity), які задають параметри передачі для кожного з'єднання. Для того, щоб організувати VoLTE потрібна підтримка двох QCI: 1 та 5. QCI 1 призначений для передачі голосу, а QCI 5 – для сигнальних IMS повідомлень.

З'єднання по QCI 5 забезпечує передачу керуючих повідомлень для створення та видалення голосових сесій. При цьому використовується протокол SIP (Session Initiation Protocol). Через з'єднання по QCI 1 голосові дані передаються з використанням стека протоколів RTP/UDP/IP.

В таблиці 1 приведено порівняння якості передачі голосу в мережах LTE та 3G. Оскільки в різних технологіях використовуються різні голосові кодеки, то якісні показники різняться. VoLTE демонструє найкращі характеристики, завдяки використанню сучасних кодеків та протоколу SIP.

Таблиця 1. Якість передачі голосу та голосової ємності мережі.

	VoLTE	3G (WB-AMR)	3G (NB-AMR)
Якість	Чудова	Гарна	Задовільна
Час встановлення виклику	~ 1 сек	~ 5 сек	~ 6 сек
Звуковий сигнал	50-7000 Гц	50-7000 Гц	200-3400 Гц
Швидкість кодеку	23.85-6.6 кбіт/с	12.65-6.6 кбіт/с	12.2-4.75 кбіт/с

Підсумовуючи, можна сказати, що мережі з комутацією каналів використовують ресурси неефективно. Для зниження вартості голосової телефонії потрібно вводити в експлуатацію технологію VoLTE. Вона також полегшує управління мережею, що є ще однією перевагою. Оскільки 4G працює тільки з пакетною комутацією, то потрібно впроваджувати IMS для забезпечення голосових викликів.

Література

1. VoLTE/ViLTE + Wi-Fi-Calling — просто о сложном //[Електронний ресурс] – режим доступу: https://habr.com/ru/company/ru_mts/blog/415551/.
2. VoLTE: что это такое в телефоне или смартфоне? //[Електронний ресурс] – режим доступу: <https://androidnik.ru/chto-takoe-volte/>.
3. Передача голоса в LTE - VoLTE //[Електронний ресурс] – режим доступу: <http://anisimoff.org/lte/volte.html>.
4. Смартфоны с VoLTE: характеристики, технологии и область применения //[Електронний ресурс] – режим доступу: <https://www.kp.ru/guide/volte.html>.
- What is Voice over LTE, VoLTE //[Електронний ресурс] – режим доступу: <https://www.electronics-notes.com/articles/connectivity/4g-lte-long-term-evolution/volte-voice-over-lte.php>.
5. IMS //[Електронний ресурс] – режим доступу: <https://uk.wikipedia.org/wiki/IMS>.
6. AMR (Сжатие звука) //[Електронний ресурс] – режим доступу: [https://ru.wikipedia.org/wiki/AMR_\(%D1%81%D0%B6%D0%B0%D1%82%D0%B8%D0%B5_%D0%B7%D0%B2%D1%83%D0%BA%D0%B0\)](https://ru.wikipedia.org/wiki/AMR_(%D1%81%D0%B6%D0%B0%D1%82%D0%B8%D0%B5_%D0%B7%D0%B2%D1%83%D0%BA%D0%B0)).

**DESIGN AND OPTIMIZATION OF COAXIAL-FED
RECTANGULAR PATCH ANTENNA FOR 2.4 GHZ FREQUENCY BAND**

Trubarov I.V.

*National Technical University of Ukraine
“Igor Sikorsky Kyiv Polytechnic Institute”
E-mail:trubarov.i@gmail.com*

**Проектування та оптимізація прямокутної патч-антени
з коаксіальним живленням для частотного діапазону 2,4 ГГц**

Здійснено проектування та оптимізацію прямокутної патч-антени з коаксіальним живленням діапазону 2.4 ГГц. Проведено моделювання роботи антени методом скінчених елементів в діапазоні робочих частот 2.4...2.483 ГГц. В результаті оптимізації антени збільшено смугу її пропускання, відкореговано резонансну частоту випромінювача так, щоб вона відповідала середині робочого діапазону, а також покращено узгодження на даній частоті. В межах робочої смуги частот КСВ розрахованої антени знаходиться в діапазоні 1...1.45.

Fast development of mobile communication systems and IoT-devices, as well as growth of the number of corresponding equipment increase the demand for small-size and high-performance microwave antennas. At present, theory of antenna design is well-studied part of microwave engineering, and there are a large number of small-size antenna types and design techniques that can be used for designing and fabrication of them [1] – [3]. Nowadays, antenna design is usually an iterative procedure involving numerous simulations and optimization of its structure. Most frequently used numerical techniques for the full field simulation of antenna structures are the finite-element method (FEM) and the finite-difference time-domain method (FDTD). The comparison of microstrip filter design using different numerical techniques was previously done in [4]. The comparison of the analytical model and the FEM simulation was done in [5] for the example of the 2.4 GHz patch antenna.

In this paper, a microstrip rectangular coaxial-fed patch antenna for the 2.4 GHz band is designed and simulated using the finite-element method. At first, the dimensions of the antenna were calculated, then the series of FEM simulations of the antenna model was done in order to achieve the best performance.

The antenna to be designed should operate in the frequency range 2400...2483 MHz, which is one of Wi-Fi frequency bands. Thus, the operating frequency of the antenna was chosen to be $f_0 = 2442$ MHz, which is the central frequency of the operating band.

To enhance the antenna bandwidth, the air was used as a dielectric between the ground plane and the patch. Aluminium was chosen as a material of which conducting parts of the antenna are made. Thus, the parameters of the layers are as

follows: dielectric constant $\epsilon_r = 1$; thickness $h = 6$ mm; thickness of the top and bottom aluminium layers $t = 0.5$ mm.

The topology of the antenna with the dimensions of the patch is depicted in Fig. 1. The antenna was designed so as to be fed by coaxial line. To perform the matching between the coaxial feeder and the radiating rectangular patch, the end of the coaxial probe should connect to the patch at the point at which its input impedance is equal to the characteristic impedance of the coaxial feeder.

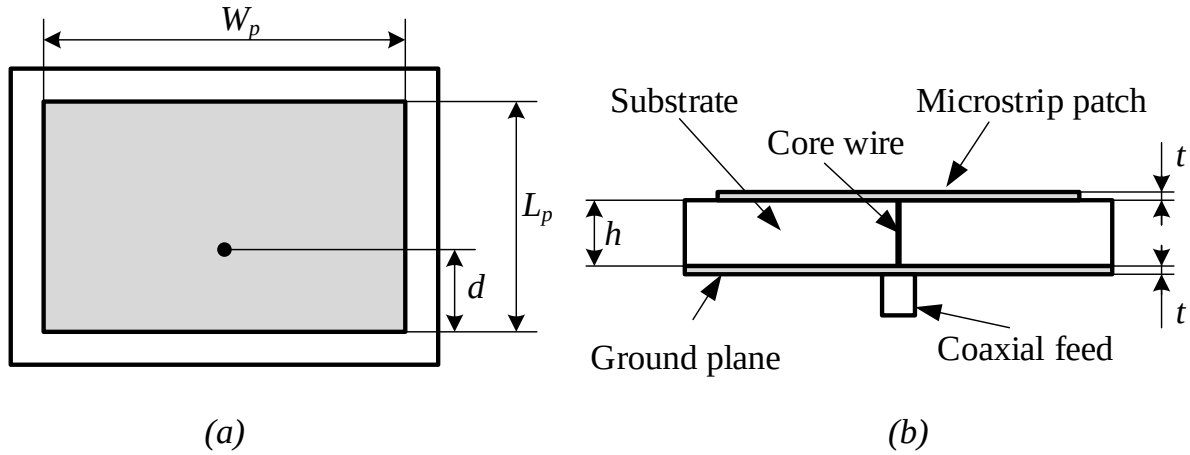


Fig.1. Dimensions of a microstrip patch antenna. (a) Dimensions of the microstrip patch. (b) Dimensions of the substrate and aluminium layers.

The design procedure described in [1] was used to obtain the initial values of the dimensions of the patch, which are as follows: width of the patch $W_p = 61.43$ mm; length of the patch $L_p = 53.18$ mm; inset distance $d = 18.07$ mm. As a coaxial feed, the model of SMA connector was used. Thus, the inset distance should correspond to the point at which the input impedance of the patch is equal to $Z_0 = 50 \Omega$.

These values were used for preparing the 3D model of the antenna shown in Fig. 2. The HFSS software was used for preparing the model and further full field simulations using finite-element numerical method.

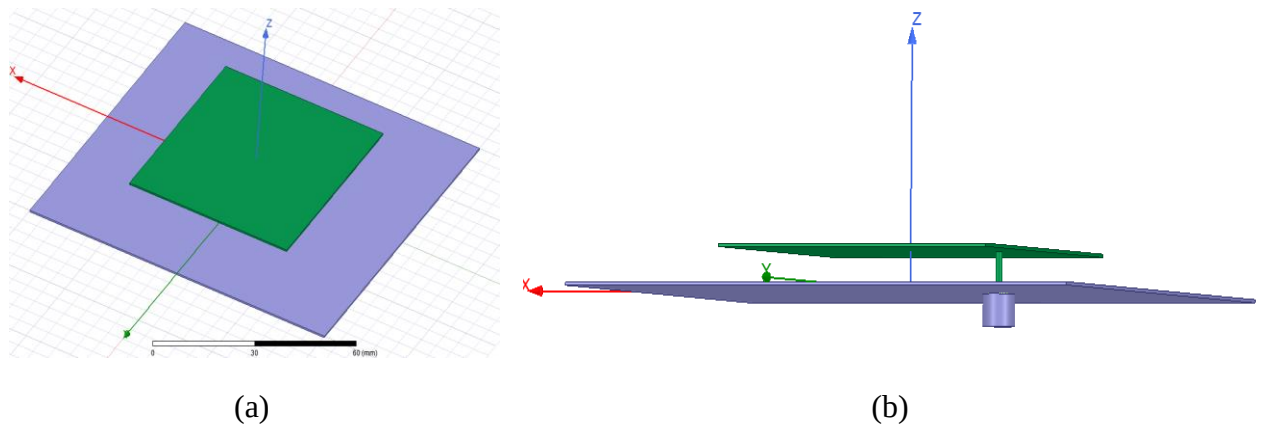


Fig.2. Model of the antenna. (a) Upper view. (b) Side view.

During the optimization the inset distance d was firstly changed to perfectly match the 50Ω coaxial feeding line with the patch. The length of the patch L_p was

also altered to adjust the resonance frequency of the patch to the value of $f_0 = 2442$ MHz.

After the optimization procedure the following dimensions were chosen for the antenna: $W_p = 62$ mm; $L_p = 53.4$ mm; $d = 9$ mm. In Fig.3, the simulated results for the directivity diagram and the frequency responses of the antenna are shown. As it could be seen, the return loss is $RL = |S_{11}| \approx -15$ dB at the edges of the operating bandwidth, i.e. at the frequencies $f_L = 2.4$ GHz and $f_R = 2.483$ GHz, and $RL = |S_{11}| \approx -66$ dB at the centre frequency $f_0 = 2.442$ GHz. The gain of the antenna is $G = 9.07$ dB. The polarization of the antenna is linear with $\mathbf{E}$ vector oriented in XZ-plane, as shown in Fig. 2.

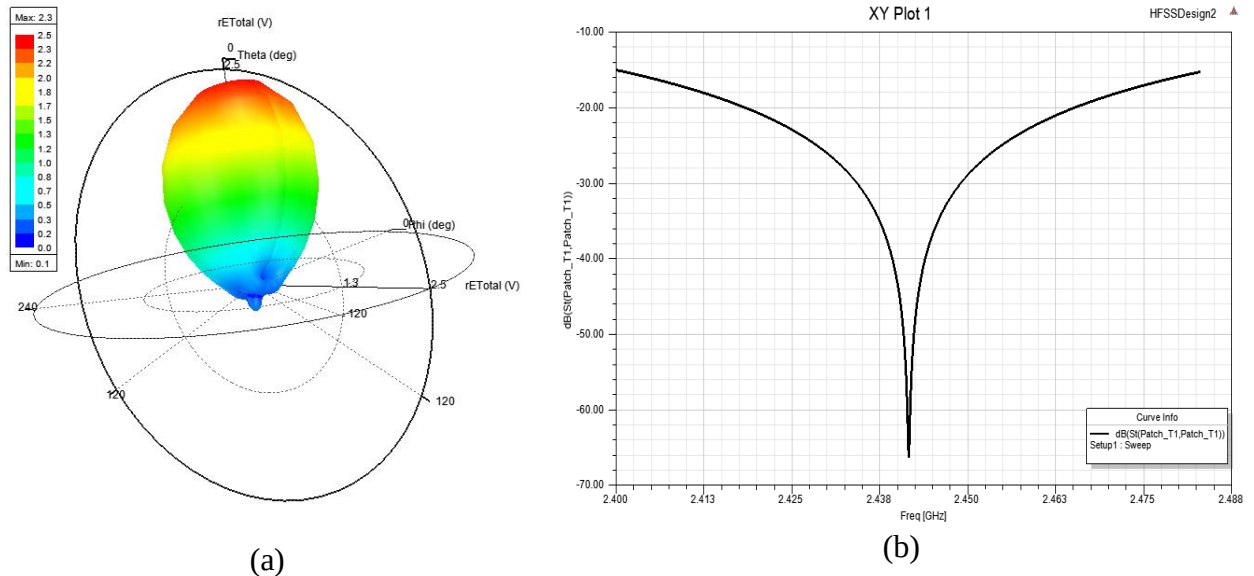


Fig.3. Characteristics of the antenna. (a) Directivity. (b) Return loss.

The antenna designed in the present research is small-sized and easily fabricated. The relatively high dielectric substrate height $h = 6$ mm as well as small value of dielectric constant $\varepsilon = 1$ lead to the relatively high bandwidth of the antenna comparing with the one studied in [5]. The bandwidth at the level of $RL = -15$ dB is $\Delta f = 83$ MHz, i.e. VSWR within the required bandwidth is in the range 1...1.45.

References

1. Balanis C. A. Antenna theory: analysis and design. – John wiley & sons, 2016.
2. Garg R. et al. Microstrip antenna design handbook. – Artech house, 2001.
3. Kumar G., Ray K. P. Broadband microstrip antennas. – Artech house, 2003.
4. Zelepukina T.V., Nemchenko K.V., Trubarov I.V., Avdeyenko G.L. *Design of microwave wideband microstrip filters using different numerical methods* // XI International Scientific Conference "Modern Challenges in Telecommunications" MCT-2017. Conference proceedings. Kyiv. Igor Sikorsky Kyiv Polytechnic Institute. – <http://conferenc.its.kpi.ua/proc/article/view/101285>.
5. Trubarov I.V. Design and optimization of microstrip patch antenna for 2.4 GHz frequency band. // XIII International Scientific Conference "Modern Challenges in Telecommunications" MCT-2019. Conference proceedings. Kyiv. Igor Sikorsky Kyiv Polytechnic Institute. – <http://conferenc.its.kpi.ua/proc/article/view/167248>.

DESIGN OF A MICROSTRIP FILTER FOR 5 GHZ BAND USING DIFFERENT NUMERICAL METHODS

Trubarov I.V.

*National Technical University of Ukraine
“Igor Sikorsky Kyiv Polytechnic Institute”
E-mail:trubarov.i@gmail.com*

Проектування мікросмужкового фільтра діапазону 5 ГГц з використанням різних чисельних методів розрахунку

Описано підхід до проектування мікросмужкових НВЧ-фільтрів із застосуванням різних чисельних методів розрахунку і пов'язаних з ними систем автоматизованого проектування. Здійснено розрахунок та моделювання мікросмужкового фільтра зі смугою пропускання 4850...5150 МГц. Здійснено порівняння характеристик фільтра, отриманих методами моментів, скінченних елементів та розрахованих за значеннями S-матриць відрізків ліній передачі.

Rapid development of mobile communication systems and growth of the number of corresponding equipment increase the demand for small-size and high-performance microwave filters. At present, theory of filter design is well-studied part of microwave engineering, and there are a large number of filter types and design techniques that can be used for designing and fabrication of filters [1] – [3]. Nowadays, a filter design is usually an iterative procedure involving numerous simulations and optimization of the filter structure. The comparison of microstrip filter design using different numerical techniques was previously done in [4]. The comparison of the analytical model and the FEM simulation was done in [5] for the example of the 2.4 GHz patch antenna.

In this paper, the design of a microstrip filter was performed, the filter was firstly modelled using three numerical techniques and then fabricated. The simulation results and measured values of scattering parameters were then compared.

The research task implied designing a bandpass microstrip filter operating in the frequency band 4850 – 5150 MHz. The parameters of the filter were as follows: center frequency $f_0 = 5\text{GHz}$, passband $BW = 300\text{ MHz}$; ripple within the passband 0.1 dB. In order to provide small dimensions of the filter, the hairpin topology was chosen for microstrip realization.

For the realization of the filter, the RT/Duroid 5880 laminate was used. The parameters of the material are as follows: dielectric constant $\varepsilon_r = 2.2$; thickness $h = 0.508\text{ mm}$; thickness of strip $t = 0.017\text{ mm}$; dissipation is defined by $\tan\delta = 0.0009$; height of the top shield $H = 15\text{ mm}$.

The Chebyshev response was used. To meet the listed above demands, the filter should consist of 5 hairpin resonators. Using the parameters of low-pass prototype, the parameters of the transmission line segments for the edge-coupled

structure can be calculated using the procedure given in [1]. The model of the filter was prepared using the Microwave Office software and is shown in Fig.1.

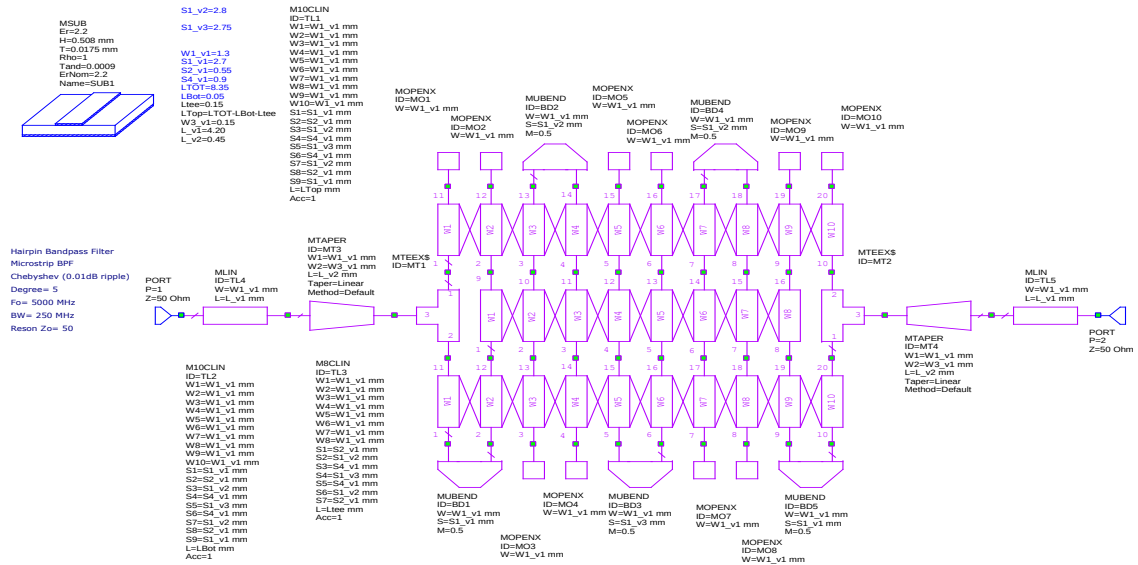


Fig.1. Model of the filter.

Using this model, the topology of the filter was generated. It was then used for preparing the 3D model for the filter shown in Fig. 2(a). This model was used to perform FEM simulation with HFSS software. Using 3D model, the prototype of the filter was fabricated as shown in Fig. 2(b). The dimensions of the filter are $25 \times 20 \text{ mm}^2$.

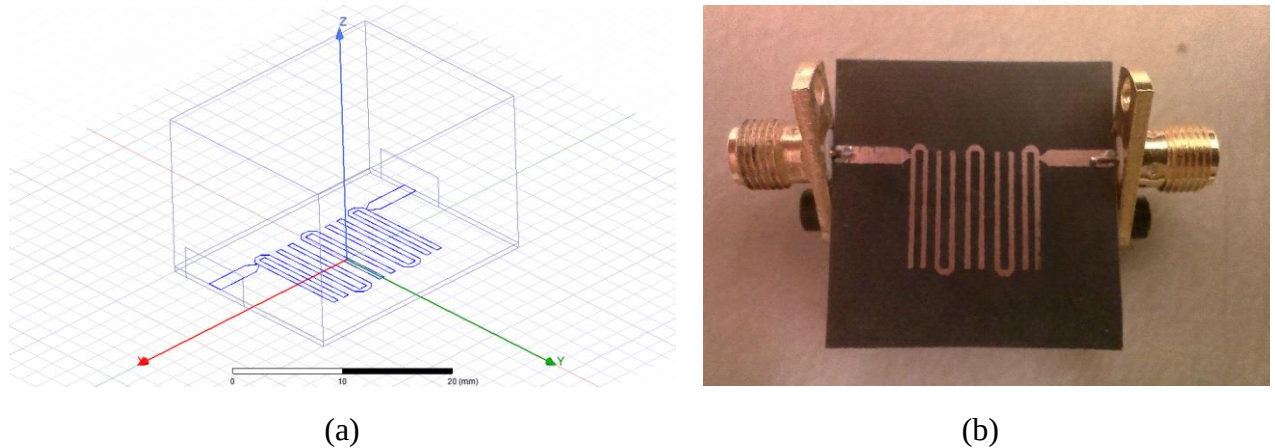


Fig.2. Topology of the filter. (a) HFSS model. (b) Fabricated filter.

In Fig.3, the simulated and measured results for the insertion loss (IL) and return loss (RL) frequency responses of the filter are shown. There are 5 curves for each characteristic: 3D FEM simulation (denoted as “HFSS”), the measured values of physical prototype (“Measured”), S-matrix calculation using the model shown in Fig. 1 (“iFilter”), MoM simulation using EMSight solver (“EMSight”) and MoM simulation using AXIEM solver (“Axiem”). It can be seen that there is a considerable difference in frequency responses for the three methods exists.

The method based on the S-matrix theory is based on lumped-element network representation of microwave structures and is then the least precise amongst the three compared methods. The MoM is 2.5D technique, which can be implemented only for planar structures, i.e. the structures consisting of a few layers. FEM is 3D technique, where the accuracy of the results can be increased by increasing the number of the cells (of tetrahedral shape). FEM method is the most precise among the three considered techniques.

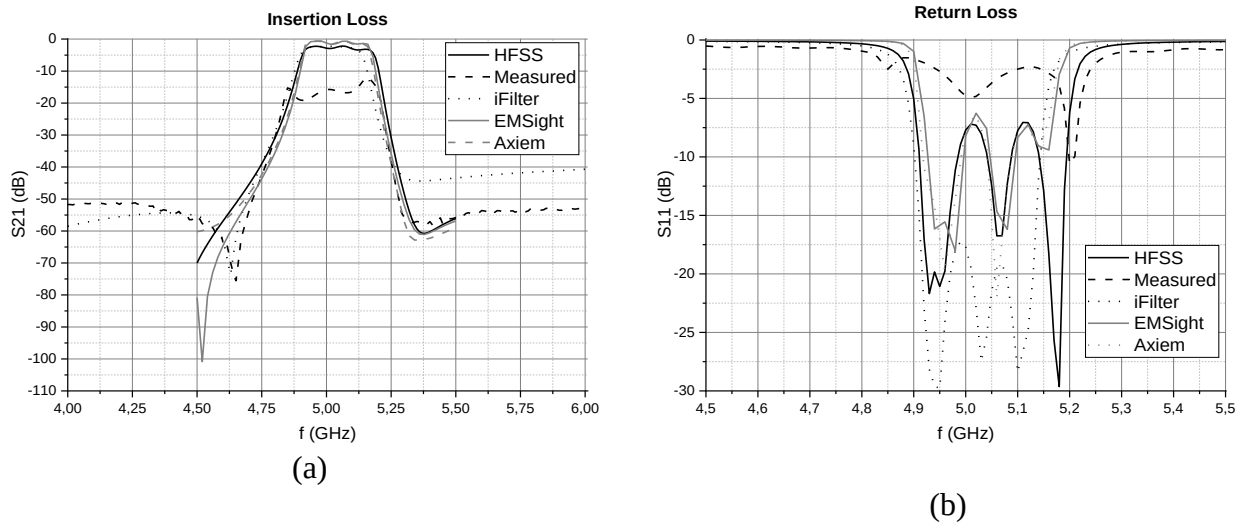


Fig.3. Frequency responses of the filter calculated by different numerical techniques.
(a) Insertion loss. (b) Return loss.

As it can be seen from Fig. 3, the S-matrix method is the fastest among others, but showing the least accuracy. MoM and FEM simulations give more precise results. The measured characteristics of the fabricated filter prototype don't show the best filter performance as given by simulations. This can be explained by the absence of the metal shield box and the shortcomings of the fabrication technique, which was insufficiently precise for the selected relatively high frequency band.

References

1. Hong J.-S. Microstrip filters for RF/microwave application, 2nd Edition. – N.Y. John Wiley and Sons, 2011.
2. Zhu, Lei, Sheng Sun, and Rui Li. Microwave bandpass filters for wideband communications. Vol. 232. – John Wiley & Sons, 2011.
3. P. Jarry and J. Beneat. Advanced design techniques and realizations of microwave and RF filters. – John Wiley & Sons, 2008.
4. Zelepukina T.V., Nemchenko K.V., Trubarov I.V., Avdeyenko G.L. Design of microwave wideband microstrip filters using different numerical methods // XI International Scientific Conference "Modern Challenges in Telecommunications" MCT-2017. Conference proceedings. Kyiv. Igor Sikorsky Kyiv Polytechnic Institute. – <http://conferenc.its.kpi.ua/proc/article/view/101285>.
5. Trubarov I.V. Design and optimization of microstrip patch antenna for 2.4 GHz frequency band. // XIII International Scientific Conference "Modern Challenges in Telecommunications" MCT-2019. Conference proceedings. Kyiv. Igor Sikorsky Kyiv Polytechnic Institute. – <http://conferenc.its.kpi.ua/proc/article/view/167248>.

DESIGN AND OPTIMIZATION OF COAXIAL-FED CIRCULAR PATCH ANTENNA FOR 2.4 GHZ FREQUENCY BAND

Trubarov I.V.

*National Technical University of Ukraine
“Igor Sikorsky Kyiv Polytechnic Institute”
E-mail: trubarov.i@gmail.com*

Проектування та оптимізація круглої патч-антени з коаксіальним живленням для частотного діапазону 2,4 ГГц

Здійснено проектування та оптимізацію круглої патч-антени з коаксіальним живленням діапазону 2.4 ГГц. Проведено моделювання роботи антени методом скінченних елементів в діапазоні робочих частот 2.4...2.483 ГГц. В результаті оптимізації, відкореговано резонансну частоту випромінювача так, щоб вона відповідала центральній частоті робочого діапазону, а також покращено узгодження на даній частоті, чим було досягнуто збільшення робочої смуги частот антени. КСВ розрахованої антени знаходиться в діапазоні 1...1.5 у робочій смузі частот.

Fast development of mobile communication systems and IoT-devices, as well as growth of the number of corresponding equipment increase the demand for small-size and high-performance microwave antennas. At present, theory of antenna design is well-studied part of microwave engineering, and there are a large number of small-size antenna types and design techniques that can be used for designing and fabrication of them [1] – [3]. Nowadays, antenna design is usually an iterative procedure involving numerous simulations and optimization of its structure. Most frequently used numerical techniques for the full field simulation of antenna structures are the finite-element method (FEM) and the finite-difference time-domain method (FDTD). The comparison of microstrip filter design using different numerical techniques was previously done in [4]. The comparison of the analytical model and the FEM simulation was done in [5] for the example of the 2.4 GHz patch antenna.

In this paper, a circular coaxial-fed patch antenna for the 2.4 GHz band is designed and simulated using the finite-element method. In order to achieve the best performance, the dimensions of the antenna were calculated, and then the series of FEM simulations of the antenna model was done.

The antenna to be designed should operate in the frequency range 2400...2483 MHz, which is one of Wi-Fi frequency bands. Thus, the operating frequency of the antenna was chosen to be $f_0 = 2442$ MHz, which is the central frequency of the operating band.

To enhance the antenna bandwidth, the air was used as a dielectric between the ground plane and the patch. Aluminium was chosen as a material of which conducting parts of the antenna are made. Thus, the parameters of the layers are as follows: dielectric constant $\varepsilon_r = 1$; thickness $h = 6$ mm; thickness of the top and bottom aluminium layers $t = 0.5$ mm.

The topology of the antenna with the dimensions of the patch is depicted in Fig. 1. The antenna was designed so as to be fed by coaxial line. To perform the matching between the coaxial feeder and the radiating circular patch, the end of the coaxial probe should connect to the patch at the point at which its input impedance is equal to the characteristic impedance of the coaxial feeder.

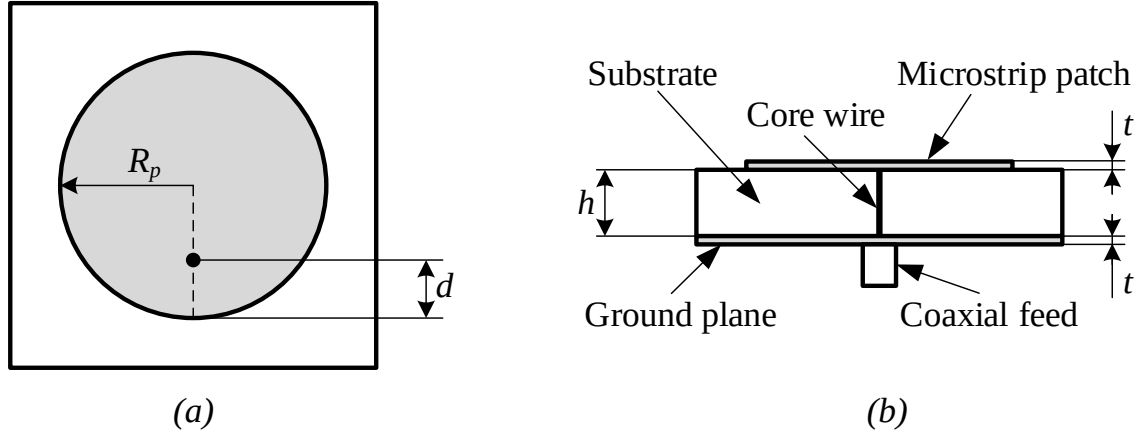


Fig.1. Dimensions of a microstrip patch antenna. (a) Dimensions of the microstrip patch. (b) Dimensions of the substrate and aluminium layers.

The patch geometry is characterized by only one parameter: radius of the patch. The design procedure described in [1] was used to obtain its initial value that turned out to be $R_p = 30.14$ mm. As a coaxial feed, the model of SMA connector was used. Thus, the inset distance should correspond to the point at which the input impedance of the patch is equal to $Z_0 = 50 \Omega$.

These values were used for preparing the 3D model of the antenna shown in Fig. 2. The HFSS software was used for preparing the model and further full field simulations using finite-element numerical method.

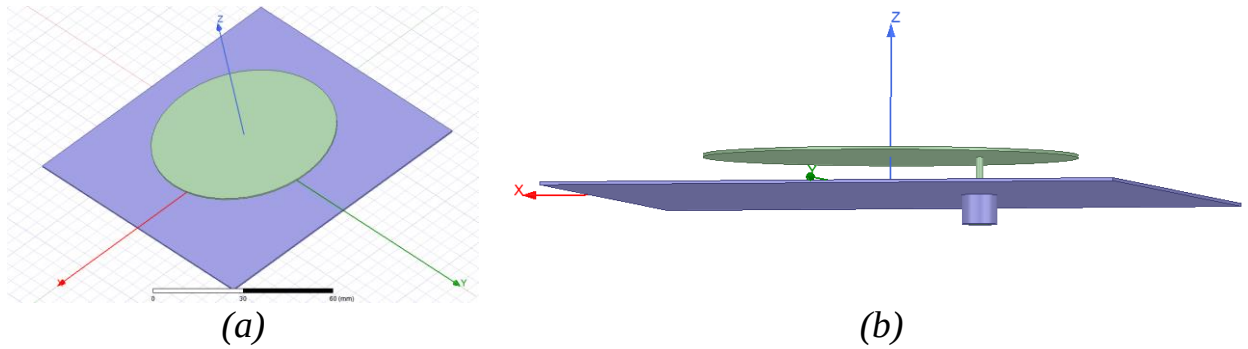


Fig.2. Model of the antenna. (a) Upper view. (b) Side view.

During the optimization the inset distance d was firstly changed to perfectly match the 50Ω coaxial feeding line with the patch. The length of the patch L_p was also altered to adjust the resonance frequency of the patch to the value of $f_0 = 2442$ MHz.

After the optimization procedure the following dimensions were chosen for the antenna: $R_p = 32$ mm; $d = 16.5$ mm. In Fig.3, the simulated results for the directivity diagram and the frequency responses of the antenna are shown. As it

could be seen, the return loss is $RL = |S_{11}| \approx -14$ dB at the lower frequency $f_L = 2.4$ GHz of the operating frequency band and $RL = |S_{11}| \approx -17$ dB at the higher frequency $f_R = 2.483$ GHz, and $RL = |S_{11}| \approx -61$ dB at the resonance frequency $f_0 = 2.449$ GHz which is slightly different from the centre frequency of the band $f_c = 2.442$ GHz. The gain of the antenna is $G \approx 8.9$ dB. The polarization of the antenna is linear with $\mathbf{E}$ vector oriented in XZ-plane, as shown in Fig. 2.

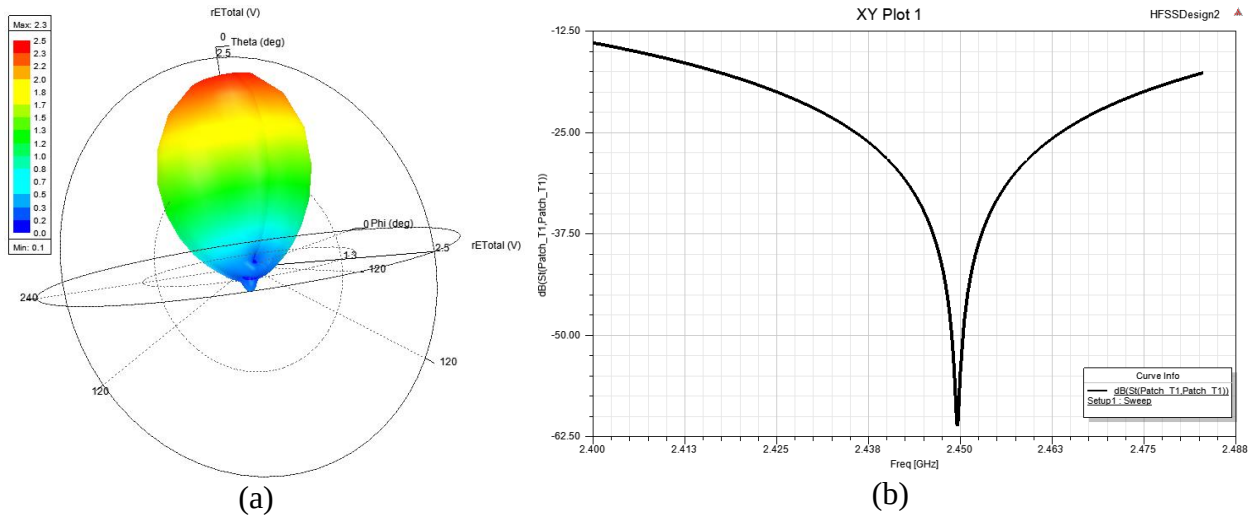


Fig.3. Characteristics of the antenna. (a) Directivity. (b) Return loss.

The key parameters of the designed antenna, namely bandwidth, gain and directivity pattern are close to those of the rectangular patch antenna with the same initial conditions. The relatively high dielectric substrate height $h = 6$ mm as well as small value of dielectric constant $\epsilon = 1$ lead to the relatively high bandwidth of the antenna comparing with the one studied in [5]. The designed antenna provides the matching of $VSWR = 1 \dots 1.5$ within the operating frequency band 2.4...2.483 GHz.

References

1. Balanis C. A. Antenna theory: analysis and design. – John Wiley & sons, 2016.
2. Garg R. et al. Microstrip antenna design handbook. – Artech house, 2001.
3. Kumar G., Ray K. P. Broadband microstrip antennas. – Artech house, 2003.
4. Zelepukina T.V., Nemchenko K.V., Trubarov I.V., Avdeyenko G.L. *Design of microwave wideband microstrip filters using different numerical methods* // XI International Scientific Conference "Modern Challenges in Telecommunications" MCT-2017. Conference proceedings. Kyiv. Igor Sikorsky Kyiv Polytechnic Institute. – <http://conferenc.its.kpi.ua/proc/article/view/101285>.
5. Trubarov I.V. Design and optimization of microstrip patch antenna for 2.4 GHz frequency band. // XIII International Scientific Conference "Modern Challenges in Telecommunications" MCT-2019. Conference proceedings. Kyiv. Igor Sikorsky Kyiv Polytechnic Institute. – <http://conferenc.its.kpi.ua/proc/article/view/167248>.

ПРИЗНАЧЕННЯ ТА ЗАДАЧІ СИСТЕМ МОНІТОРИНГУ ДЖЕРЕЛ РАДІОВИПРОМІНЮВАННЯ НА БАЗІ ВИКОРИСТАННЯ ПРИСТРОЇВ SDR

Ігнатченко М.М., Авдєєнко Г.Л.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: ignatchenkomaxim@gmail.com, django2006@ukr.net

Destination and tasks of the radio sources monitoring based on SDR devices application

This article is devoted to the fundamental concepts of radio sources monitoring systems based on SDR devices application. Their tasks are also shown at the block diagram of such systems using a specific example of monitoring system named “Armada”.

Апаратура автоматизованих систем радіомоніторингу (АСРМ) отримала широке застосування як інструмент вирішення завдань в самих різних областях: від управління використанням радіочастотного спектру РЧС до контролю електромагнітної обстановки (ЕМО).

У той же час у світі набувають широкого поширення пристрої програмно-керованого радіо (SDR) різних виробників, такі як RTLSDR, Nuand BladeRF, HackRF, USRP, широкі функціональні можливості яких роблять їх привабливими для використання у АСРМ різних рівнів. Тому розглянемо варіанти застосування SDR у АСРМ для контролю ЕМО.

Основними функціями АСРМ є постійне або періодичне спостереження за ефіром в широкому діапазоні частот, оперативне виявлення, аналіз і локалізація потенційних або спеціально організованих радіоканалів витоку інформації і проведення інших заходів з протидії знімання інформації в контрольованих зонах (приміщеннях) різних відомств і комерційних установ. Зокрема, апаратура АРМ дозволяє перевіряти радіотехнічні пристрої та обчислювальну техніку на наявність і рівень побічних електромагнітних випромінювань та наведень (ПЕМВН), що представляють інтерес для перехоплення радіозасобами, а потім і оцінювати ефективність заходів щодо запобігання електромагнітного доступу до конфіденційних даних (наприклад, екранування, зашумлення) [1].

Узагальнена структурна схеми АСРМ на прикладі АСРМ “Армада” [2] зображена на рис.1. Головним елементом АСРМ, які відповідно до рис.1 виконують моніторинг ЕМО, пеленгування джерел радіовипромінювання (ДРВ) є широка номенклатура портативних, мобільних та стаціонарних станцій, у складі яких є один або декілька ширококутових скануючих радіоприймачів. Враховуючи ширококутовість сучасних SDR приймачів (наприклад, SDR радіоприймач Nuand BladeRF має смугу робочих частот 0,3...3,8 ГГц, а SDR радіоприймач HackRFOne – 0,001...6 ГГц) а також можливість оперативної реалізації більшості основних функцій скануючого радіоприймача (підсилення, фільтрація, демодуляція, переналаштування

частоти, аналіз спектру тощо) за допомогою відповідного програмного забезпечення (наприклад, MatLab, SDRSharp, SDR Console, GNURadio або будь-яких інших програм, що написані на мові програмування Python), спрощену структурну схему мобільної або стаціонарної станції радіомоніторингу можна представити як сукупність антенної системи та M -ої кількості SDR приймачів, які своїми радіочастотним інтерфейсом за допомогою коаксіальних кабелів підключаються до антенної системи, а своїми цифровими USB інтерфейсами – до одного або декількох персональних комп'ютерів (рис.2).

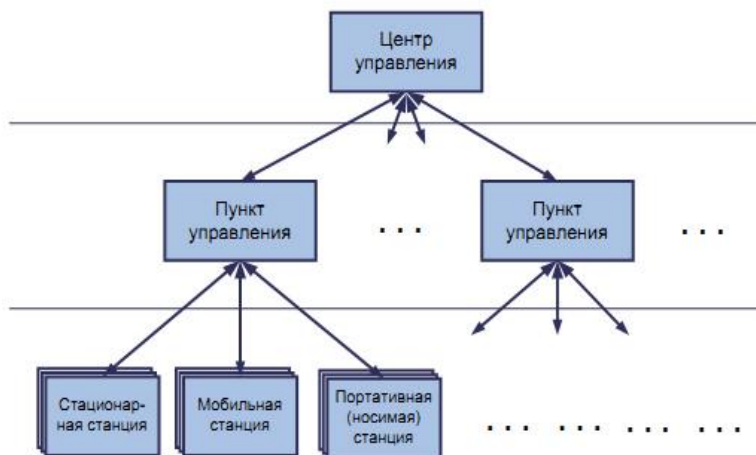


Рис. 1. Структурна схема АСРМ «Армада».

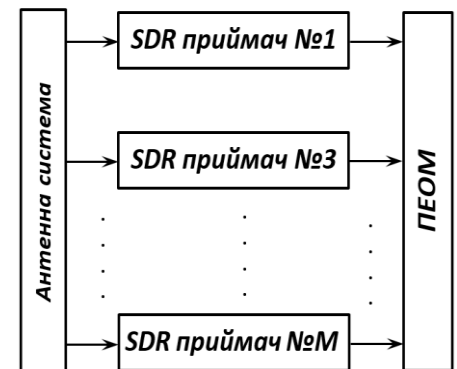


Рис.2. Структурна схема мобільної (стаціонарної) станції радіомоніторингу на основі застосування SDR приймачів.

Основні функції АСРМ з використанням SDR пристроїв можуть бути розбиті на наступні основні групи:

- універсальні функції, виконання яких, як правило, забезпечується сучасними АСРМ;
- додаткові функції вирішення завдань радіомоніторингу на місцевості;
- додаткові функції вирішення завдань радіомоніторингу в одному окремо контрольованому приміщенні і групі найбільш важливих приміщень, розміщених на контрольованому об'єкті;
- додаткові функції виявлення ПЕМВН.

До універсальних функцій засобів радіомоніторингу, що можуть бути реалізовані з використанням SDR пристроїв відносяться:

- панорамний спектральний аналіз в реальному часі з максимальною високою швидкістю, роздільною здатністю і адаптацією до складної електромагнітної обстановки;
- швидкий пошук «нових» випромінювань в тому числі широкосмугових, та випромінювань з динамічною частотно-часовою структурою, вимір їх параметрів, порівняння з базою даних для визначення їх небезпеки (цінності) для користувача;
- створення баз даних, поповнення їх і зіставлення зареєстрованих даних з еталонами, що зберігаються в базах;
- контроль ДРВ з оцінкою характеристик випромінювання;

- запис радіосигналів, в тому числі цифрових, одночасно зі службовими параметрами (частота, час, рівень сигналу, спектрограма і т.п.) і подальше їх відтворення;

- технічний аналіз радіосигналів в реальному часі і при відкладеній обробці.

До додаткових функцій рішення задач радіомоніторингу на місцевості, що можуть бути вирішені при використанні в АСРМ пристроїв SDR слід віднести:

- вимір напруженості поля або щільності потоку потужності;
- пеленгація ДРВ з довільними видами модуляції по азимуту і куту місця;

- визначення положення стаціонарних і мобільних ДРВ на місцевості і в протяжних об'єктах, відображення їх на картографічному фоні (цифровому зображенні об'єкта).

Також SDR пристрої можуть бути застосовані для вирішення завдань радіомоніторингу в одному і кількох контрольованих приміщеннях:

- пошук і виявлення технічних каналів витоку інформації в одному або декількох приміщеннях;

- ідентифікація приналежності ДРВ до радіомікрофонів;

- локалізація розташування ДРВ.

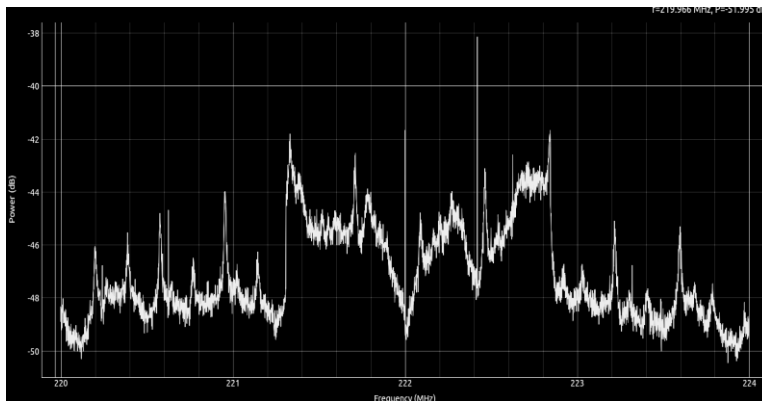


Рис.3. Моніторинг спектру сигналу цифрового радіомовлення стандарту DAB+ на частоті 11D.

На рис.3 показано результати моніторингу спектру сигналу цифрового радіомовлення стандарту DAB+, що здійснювався в реальному масштабі часу на частоті 11D (222,064 МГц) за допомогою антени типу «хвильовий канал» та SDR приймача RTLSDR, що був підключений до ПК з операційною системою

Ubuntu 19.04. Спектр було отримано у програмі Qspectrumanalyzer, яка дозволяє досліджувати спектри прийнятих сигналів як в усьому діапазоні роботи SDR приймача, так й у його окремих смугах.

Отже, SDR пристрої завдяки своїй універсальності та функціональності, що досягається в можливості зміни їх програмного забезпечення без зміни їх апаратної частини, можуть бути використані для реалізації більшості функцій, пов'язаних з обробкою сигналів в сучасних АСРМ, наприклад, в якості панорамних аналізаторів спектрів або демодуляторів сигналів.

Література

1. Рембовский А.М., Ашихмин А.В., Козьмин В.А. Радиомониторинг: задачи, методы, средства. — М.: Горячая линия-Телеком, 2010. — 624 с.
2. Автоматизированная система радиомониторинга "АРМАДА"/[Електронний ресурс] — режим доступу: <http://www.bnti.ru/des.asp?itm=5933&tbl=04.01.01.02.01>.

ЗАСТОСУВАННЯ ТРАНСИВЕРУ NUAND BLADERF x40 SDR ДЛЯ ФОРМУВАННЯ ТЕЛЕВІЗІЙНИХ СИГНАЛІВ СТАНДАРТУ DVB-S2

Авдєєнко Г.Л., Мар'яненко А. О.

Інститут телекомунікаційних систем КІП ім. Ігоря Сікорського, Україна

E-mail: djang02006@ukr.net, blaze.of.insomnia@gmail.com

Application of Nuand BladeRF x40 SDR transceiver for generating television signals of DVB-S2 standard

This article highlights the main benefits of using a DVB-S2 satellite TV standard. DVB-S2 digital television signal generation from a multi-program transport TV stream using Nuand BladeRF x40 SDR transceiver operating under the GNURadio software environment was considered.

Як і будь-яка високотехнологічна сфера діяльності, супутниковий зв'язок знаходиться у стані постійної трансформації та розвитку. Збільшення кількості і якості каналів – призвело до підвищення навантаження на передаюче обладнання супутника, що змусило більшість європейських операторів супутникових систем прямого мовлення зробити поетапний перехід до застосування стандарту DVB-S2 замість стандарту DVB-S. Стандарт DVB-S2 з точки зору вибору параметрів для формування сигналу має більшу гнучкість, а також забезпечує такі переваги перед DVB-S:

- більш потужна система кодування, заснована на кодах Боуза-Чоудхурі-Хоквінгема (БЧХ-коди) та кодах з малою щільністю перевірок на парність (LDPC);
- розширені формати модуляції (QPSK, 8-PSK, 16-APSK, 32-APSK);
- розширені формати швидкості попередньої корекції помилок (FEC) (1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 5/6, 8/9 і 9/10), що дозволяє забезпечити прийом сигналу (FEC = 1/4; 1/3; 2/5) у поганих умовах прийому, тобто для малих значень співвідношення сигнал / шум (SNR);
- покращений коефіцієнт згортання $\alpha = 0,25$ та $0,2$. [1]

Формування сигналу в трансиверах SDR, зазвичай, виконується програмуванням його, наприклад, за допомогою програмного середовища GNURadio або MatLab. Трансивери SDR коштують значно дешевше, ніж професійні модулятори DVB-S2, але в той же час використовують середовище GNURadio, яке забезпечує гнучку конфігурацію різних програмних вузлів (таких як кодери, цифрові фільтри тощо) модулятора, вони дозволяють більш детально розглянути особливості формування різних сигналів, включаючи цифрові телевізійні сигнали.

Метою даної доповіді є розгляд особливостей формування цифрового телевізійного сигналу DVB-S2 з багатопрограмного MPEG TS з використанням трансиверу Nuand BladeRF x40 SDR та програмного середовища GNURadio з подальшою оцінкою якості сформованого DVB-S2 сигналу.

Формування багатопрограмного телевізійного транспортного потоку (MPEG TS) здійснювалася демодуляцією та декодуванням стандартного сигналу DVB-S у супутниковому приймачі Prof Revolution S2 7500 USB, випромінюваному від геостационарного супутникового транспондера Astra 4A (орбітальне положення 4,9°E). Отриманий сигнал має наступні параметри: несуча частота $f = 11766$ МГц, горизонтальна поляризація та $SR = 27500$ Msps і $FEC = 3/4$. MPEG TS з цього сигналу записувався на жорсткий диск персонального комп'ютера (ПК) у вигляді файлу з розширенням *.ts.

Для роботи з трансивером BladeRF x40 було використано ПК з операційною системою Ubuntu версії 18.04 та встановленою на ньому бібліотекою драйверів. Підключення трансиверу BladeRF x40 до ПК здійснювалося через інтерфейс USB 3.0. [2]

В якості програмної моделі модулятора DVB-S2 в середовищі GNURadio можна використовувати готову спеціалістами SDR та радіоаматорами таку підпрограму, як *gr-dvbs2* або *gr-dtv*. Основна відмінність цих підпрограм полягає в тому, що *gr-dvbs2* використовує графічні віджети QT GUI, а *gr-dtv* використовує графічні віджети WX GUI. Узагальнена блок-схема модулятора DVB-S2 в середовищі GNURadio показана на рис.1 і включає такі елементи: 1) блок "Джерело файлу", в параметрах якого вказується шлях до файлу із записаним транспортним потоком; 2) генератор заголовків поточкових кадрів (BBHeader), 3) скремблер поточкових кадрів (BBScrambler); 4) BCH-кодер; 5) LDPC-кодер; 6) ущільнювач; 7) модулятор; 8) генератор PLP- кадрів (Physical layer Framer); 9) FFT-фільтр; 10) приймач даних (osmocom Sink).

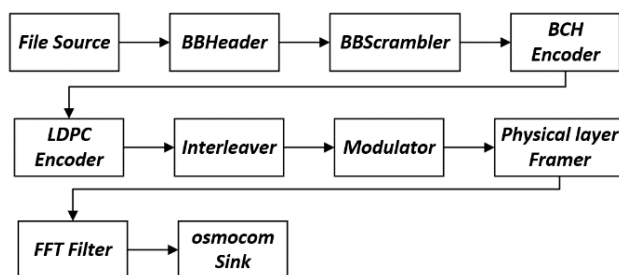


Рис. 1 Узагальнена блок-схема моделі ПЗ модулятора DVB S2 в програмному середовищі GNURadio

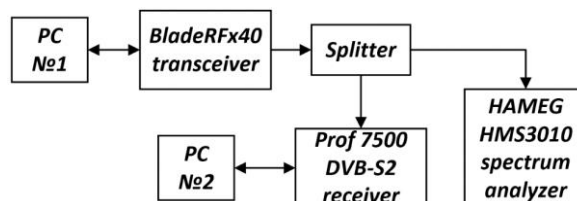
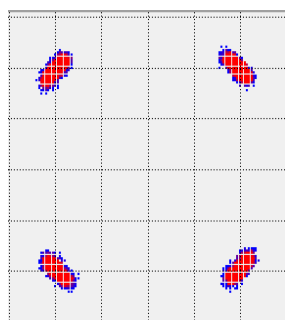


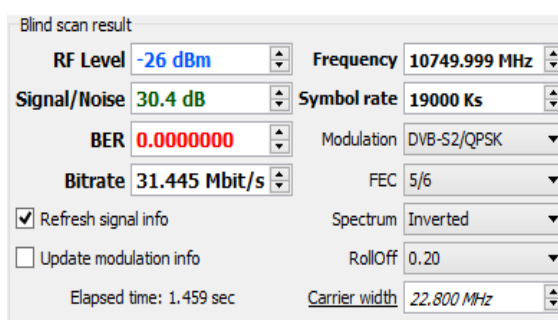
Рис. 2 Структурна схема для вимірювання параметрів сигналу DVB -S2, що сформована трансивером SDR BladeRF x40

Для формування радіосигналу DVB-S2 з MPEG TS зі швидкістю потоку 32 Мбіт/с, були встановлені в програмній моделі модулятора DVB-S2 в GNURadio наступні параметри: 1) символна швидкість 19 Msps (що відповідає 38 Мбіт/с при модуляції QPSK та 57 Мбіт/с – 8-PSK); 2) коефіцієнт згортання $\alpha = 0,2$; 3) кількість відводів цифрового фільтра дорівнює 200; 4) модуляція - QPSK або 8-PSK; 5) швидкість кодування FEC = 5/6; 6) вихідна частота $f_0 = 1000$ МГц. На рис. 2 показана блок-схема вимірювання параметрів сигналу DVB-S2, сформованого за допомогою трансиверу SDR BladeRF x40.

На рис. 3 (а) показано сигнальне сузір'я модуляції QPSK, а на рис. 3 (б) показані параметри сигналу DVB-S2, прийнятого приймачем Prof 7500, який формувався трансивером BladeRF x40 SDR.



а)



б)

Рис. 3 Сузір'я (а) та параметри сигналу QPSK DVB-S2, який формується трансивером BladeRF x40 SDR після його отримання приймачем Prof 7500 DVB-S2

На рис. 4 (а) показано сигнальне сузір'я модуляції 8-PSK, а на рис. 4 (б) показані параметри сигналу DVB-S2, прийнятого приймачем Prof 7500, який формувався трансивером BladeRF x40 SDR.

Аналіз результатів вимірювань показує низьку ймовірність бітової помилки (BER $< 10^{-8}$) після демодуляції та декодування сигналу DVB-S2, що, в свою чергу, забезпечує високу суб'єктивну якість відтворення зображення і звуку для кожного телеканалу MPEG TS.

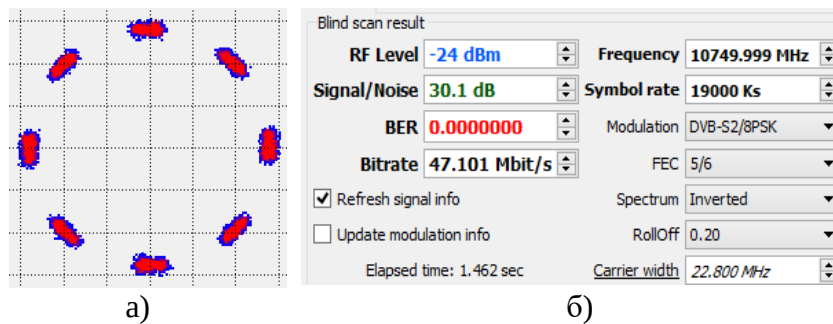


Рис. 4 Сузір'я (а) та параметри сигналу DVB-S2 8-PSK, який формується трансивером BladeRF x40 SDR після його отримання приймачем Prof 7500 DVB-S2.

Як видно з рис. 3 і рис. 4, що прийнятий сигнал приймачем Prof 7500 має SNR не менше 25 дБ, а BER $<10^{-8}$ для згортання $\alpha = 0,2$.

Цікаво також дослідити залежність таких параметрів сигналу DVB-S2 як SNR, BER від різних значень коефіцієнта згортання та FEC, типів модуляції та символної швидкості. Результати вимірювання параметрів сигналу DVB-S2 (SNR, BER, РЧ рівень), виконаного приймачем Prof 7500 для QPSK і 8-PSK модуляції, FEC = 5/6 і символною швидкістю 19 Msps для різних значень коефіцієнту згортання, який представлений у таблиці 1. Як видно з таблиці 1, спостерігається погіршення SNR, коли значення коефіцієнта згортання зменшується.

Табл. 1. Вимірювання параметрів сигналу DVB-S2 для різних значень коефіцієнту згортання.

Mod.	Parameter	roll-off factor, α						
		0.2	0.1	0.05	0.02	0.01	0.005	0.001
QPSK	SNR, dB	29.8	29.6	26.4	24.5	24.4	23.6	20.2
	BER	$<10^{-8}$	$<10^{-8}$	$<10^{-8}$	$<10^{-8}$	$<10^{-8}$	$<10^{-8}$	$<10^{-8}$
	RF level, dBm	-23	-23	-23	-23	-23	-23	-25
8-PSK	SNR, dB	29.8	29.4	26.6	24.6	24.2	23.6	23.1
	BER	$<10^{-8}$	$<10^{-8}$	$<10^{-8}$	$<10^{-8}$	$<10^{-8}$	$<10^{-8}$	$<10^{-8}$
	RF level, dBm	-25	-25	-23	-23	-23	-23	-23

Результати тестів показали можливість формування стандартного сигналу DVB-S2 із застосуванням трансиверу BladeRF x40 SDR та програмного забезпечення GNURadio, а також його успішний прийом з використанням приймача DVB-S2 із SNR не менше 29 дБ та BER не гірше ніж 10^{-8} при використанні QPSK та 8-PSK при значенні коефіцієнта згортання 0,2.

Література

1. DVB-S2. Digital Video Broadcasting (DVB); Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications; Part 2: DVB-S2 Extensions. URL:https://www.etsi.org/deliver/etsi_en/302300_302399/30230702/01.01.01_60/en_30230702v010101p.pdf.
2. Nuand BladeRF x40. URL:<https://www.nuand.com/product/bladerf-x40/>.

ПРИСТРІЙ ПЕРЕВІРКИ ДЖГУТІВ

Накоренко А.А., Губар В.Г.

Факультет електроніки КПІ ім. Ігоря Сікорського, Україна

E-mail: artemnakorenko59@gmail.com, s.gubar@kpi.ua

Cable tester

A cable tester is a device that checks all wires in a cable or harness. It consists of two independent systems - a verification unit and a control unit. This approach provides some advantages over analogues. Firstly, it is possible to quickly replace the verification unit, which makes it possible to quickly change the connectors for checking cables. Secondly, this difference makes it easy to transport the device.

Сьогодні ринок пристроїв перевірки джгутів представлений таким основними типами приладів:

- Тестери витих пар [1];
- Моноблочна конструкція, з індикацією через рідкокристалічний екран (LCD)[2];
- Моноблочна конструкція, що працює в зв'язку з ПК[3];

Перший тип пристроїв працює лише з одним типом кабелів. Другий тип має вже встановлені роз'єми для перевірки джгутів (роз'єми типу D-subminiature), що не дозволяє перевіряти кабелі з іншими типами роз'ємів; результати відображаються на рідкокристалічному екрані, що, в порівнянні з organic light emitting diode (OLED) дисплеєм, має гірший показник контрасту кольорів. Третій тип, має той же недолік, пов'язаний з представленими роз'ємами; результати індикуються на екрані комп'ютера.

Розроблюваний пристрій покликаний виправити недоліки аналогів, тобто забезпечити роботу як через ПК так і самостійно; покращити можливості для транспортування; забезпечити можливість швидкої зміни роз'ємів для перевірки різних типів джгутів.

Для досягнення цих цілей, конструкція розробленого пристрою не є моноблочною, а поділена на дві незалежні системи – блок контролю та блок перевірки. Таке рішення значно спрощує транспортування системи. Але основною перевагою є те, що це рішення дозволяє швидко змінювати блоки перевірки зі встановленими роз'ємами. Тобто зміна кількості контактів в джгуті або підключення іншого типу роз'єму, до якого підключений джгут, не потребує перепрограмування або додаткового переналаштування блоку управління.

Пристрій може працювати в двох режимах: як без комп'ютера так і з ним. В першому режимі індикація відбувається за допомогою OLED дисплею. Вибір такого типу дисплею обґрунтований кращою чіткістю та

контрастністю зображення в порівнянні з LCD- дисплеями, що важливо при роботі в не закритих приміщеннях або при яскравому освітленні[4]. Перехід між провідниками, що перевіряються, відбувається за допомогою двох кнопок, що спрацьовують за перериванням.

В другому режимі перевірка відбувається автоматично в окремій програмі, що працює через СОМ-порт. Перевірка відбувається автоматично, користувач отримує результат роботи виведений на екран. Також користувач може налаштовувати сценарії перевірки джгутів в програмі Excel.

Блок управління побудований на основі мікроконтролеру. Згідно до завдань, що виконуватиме пристрій, це може бути будь-який з мікроконтролерів серій, що підтримують інтерфейси I2C, SPI, USART. Використано плату налагоджування STM32F303RE. Використання саме готової системи викликане більшими фінансовими затратами на виготовлення власної плати та монтаж компонентів. Використання інших систем керування та обробки даних, типу FPGA не має сенсу, через невеликий об'єм даних для аналізу.

Так як пристрій передбачає перевірку джгутів з великою кількістю дротів, використовувати для цього окремі виводи мікроконтролера не є оптимальним, тому запропоновано використання розширювачів портів PCF8574, що працюють за інтерфейсом I2C.



Рис.1. Блок-схема пристрою.

При розробці виникла проблема з розширювачами. Справа в тому, що порти у PCF8574 називаються «квазі-двонаправленими». Фактично, при операції запису одного байту в PCF8574, відбувається виставлення портів введення /виведення виходячи з значення відповідного порту біта даних. Причому, якщо біт встановлений в нуль, вихід драйверу порту буде підключено до землі (2, рис. 2). Якщо біт встановлено в лог.1, вихід драйвера порту буде підключено до лінії живлення VDDE за допомогою PullUp резистора опором близько 50кОм. При напрузі живлення 5В, струм виходу

WAVEGUIDE DISTRIBUTION OF COUPLED DIELECTRIC RESONATOR MODES IN THE UNIFORM LATTICES

Trubin A. A.

National Technical University of Ukraine
 “Igor Sikorsky Kyiv Polytechnic Institute”
 E-mail: atrubin@ukrpost.net

ХВИЛЕВОДНИЙ РОЗПОДІЛ КОЛИВАНЬ ЗВ'ЯЗАНИХ ДІЕЛЕКТРИЧНИХ РЕЗОНАТОРІВ В ОДНОРІДНИХ РЕШІТКАХ

Вперше досліджено явище формування "хвильоводних" коливань в однорідних решітках діелектричних резонаторів.

Structures consisting of a large number of resonators have interesting properties that are absent in homogeneous materials. The purpose of this report is to consider a new property of DR gratings that form waveguide structures at particular frequencies of forced oscillations. Interestingly, such waveguide channels may be form in a homogeneous lattice.

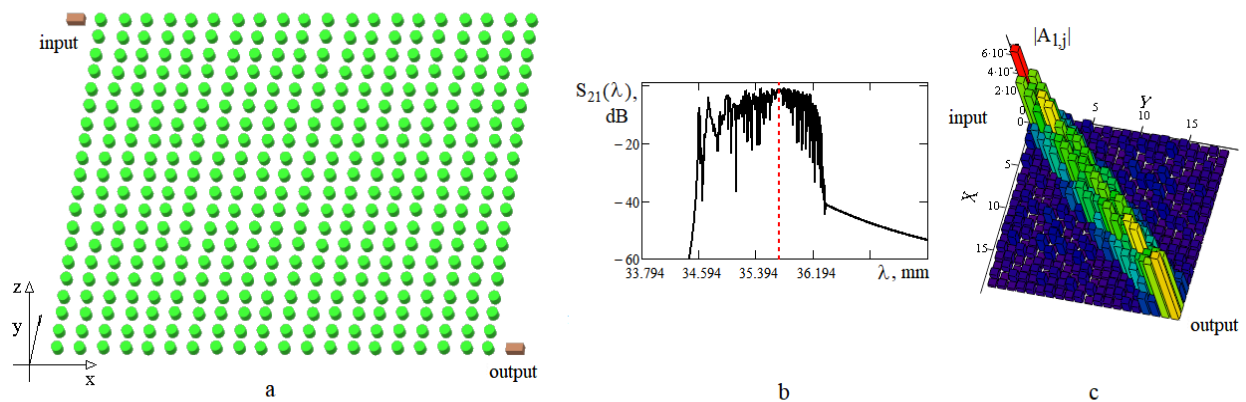


Fig. 1. Square lattice of cylindrical DRs with incoming and outgoing transmission lines (a). Dependence of the transfer coefficient between the input and output lines on the wavelength of a lattice of 400 DRs with H_{101} magnetic oscillations (b). Waveguide distribution of coupled modes on $\lambda = 35,718$ mm (c).

In this paper, we consider the conditions under which the DR coupled oscillations of a similar type are formed.

The formation of a waveguide channel was first observed on a flat square lattice of cylindrical DRs with magnetic azimuthally uniform oscillations H_{101} (Fig. 1, a). The dielectric permittivity of the DRs $\epsilon_{1r} = 81$; $1/\text{tg}\delta = 10^5$; $\Delta = L/2r_0 = 0,44$; the coupling coefficient between the DR and transmission line

$k_L = 0,02$. The coupling coefficients between the resonators was calculated by the formulas [1]. In fig. 1 shows the amplitude-frequency response of the lattice S_{21} coefficient of transmission between input (1) and output port (2). The red line marks the wavelength at which the formation of waveguide oscillations is detected. In fig. 1, c shows the distribution of the amplitude modulus of the DRs in the lattice at the wavelength of waveguide resonant oscillations.

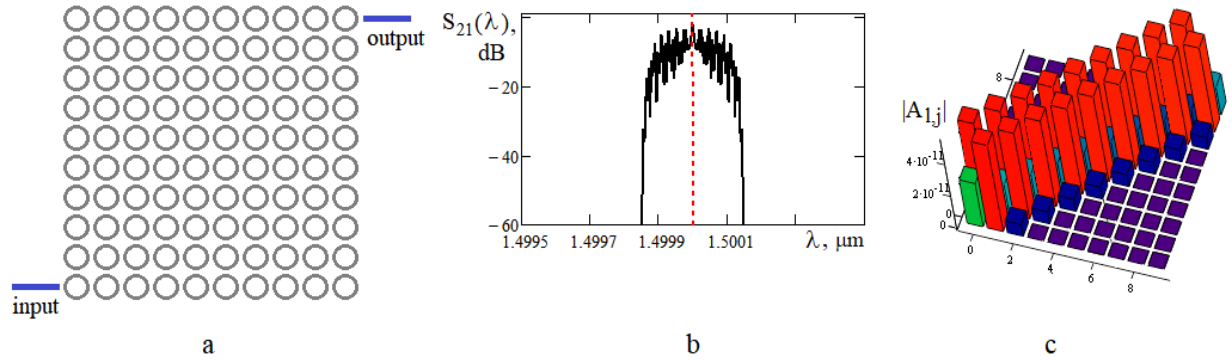


Fig. 2. Square lattice of optical microresonators (a). S-matrix coefficient between the input and output lines (b). Waveguide distribution of coupled modes on $\lambda = 1,5 \mu\text{m}$ (c).

The results of the calculation of the dependence of S_{21} on a square lattice of ring microresonators (Fig. 2, a), according to [1], are shown in Fig. 2, b. The red line also marks the wavelength at which the formation of waveguide oscillations is detected. Open space coupling coefficient of each microresonator $k_{os} = 10^{-6}$; the coupling coefficient between adjacent microresonators was $k_{j,j+1} = 5 \cdot 10^{-5}$; The coupling coefficient between the microresonators of the grating and the input (output) transmission line $k_L = 3 \cdot 10^{-4}$. Fig. 2, c shows the distribution of the amplitude modulus of the DRs in the lattice at center wavelengths.

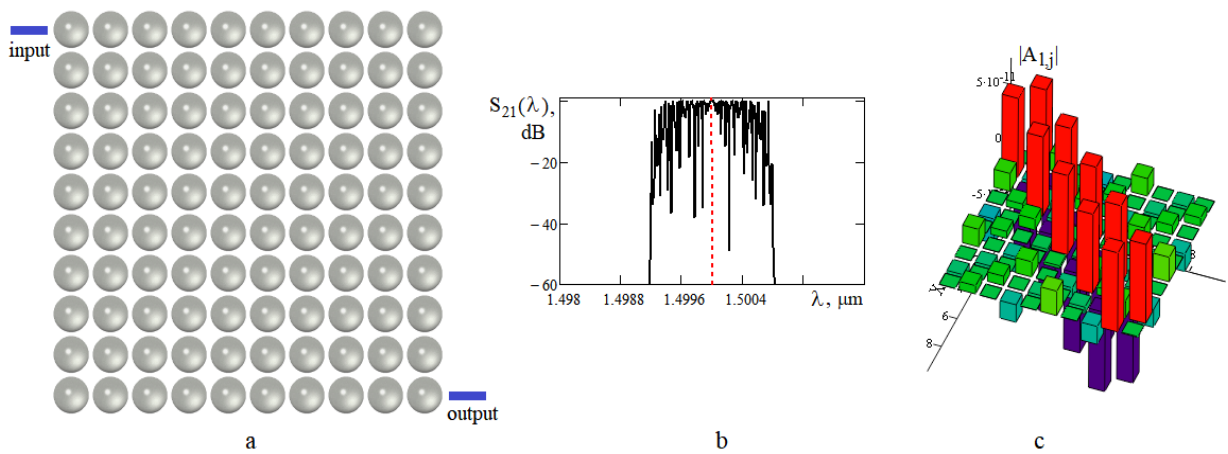


Fig. 3. Square lattice of spherical microresonators (a) with H_{mm1} ($m=30$) magnetic oscillations (a). The transfer coefficient between the input and output lines (b). Waveguide distribution of coupled microresonator modes on $\lambda = 1,5 \mu\text{m}$ (c).

In Fig. 3 shows the results of calculation of scattering on a square lattice of coupled spherical microresonators with magnetic oscillations H_{mm1} . The coupling coefficients between the microresonators was calculated by using the results [1].

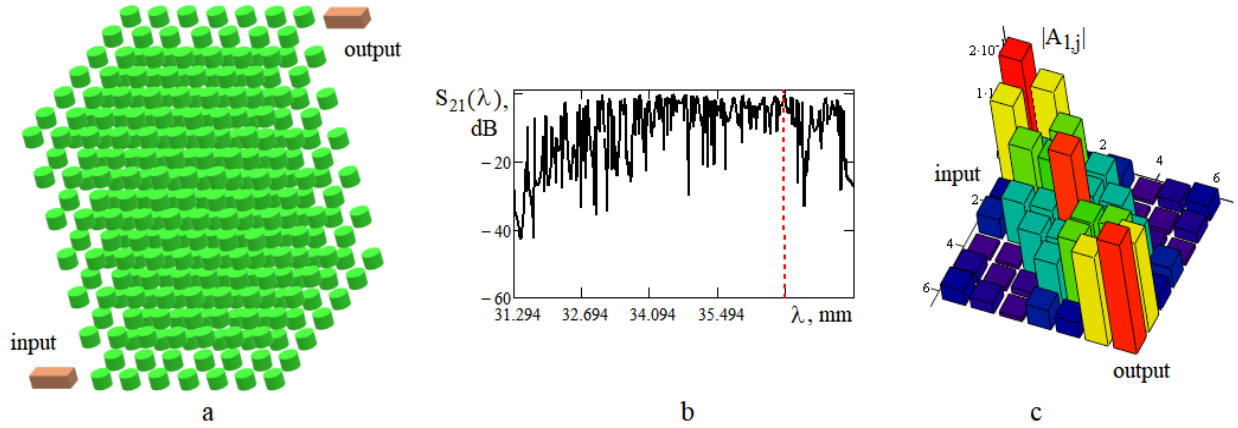


Fig. 4. 3-dimensional square lattice of DRs (a). S-matrix coefficient between the input and output lines of a lattice of 7x7x7 DRs with H_{101} magnetic oscillations (b). Waveguide distribution modes in 4 layer on $\lambda = 36,873$ mm (c).

A similar phenomenon is observed in 3-dimensional lattices. In Fig. 4, a shows a square lattice of cylindrical DRs with magnetic oscillations H_{101} . The distribution of the S matrix by wavelengths is shown in Fig. 4, b. The waveguide distribution of amplitudes was observed in each layer on the wavelength indicated by the dashed line (Fig. 4, b). Thus, we can conclude that in this case a planar waveguide is formed in the diagonal plane of the lattice. Figure 4, c shows example of distribution of the amplitude modulus in the 4 layer of the DRs lattice.

As can be seen from the data obtained, we have discovered a new phenomenon of waveguide distributions of the DR coupled modes in homogeneous two and three-dimensional square lattices. This phenomenon is quite universal in nature, since it was observed on gratings consisting of different types of resonators with different types of oscillations. In this case, the observed distribution of amplitudes is associated with forced oscillations and, in contrast to the natural oscillations of the lattice (Bloch states), is observed only at certain wavelengths. At other wavelengths, the distribution of the field is more complex.

In the future, the examined properties of the DR lattices can be used in the design of different elements of optical communication systems.

References

1. Trubin A.A. Lattices of Dielectric Resonators, Springer International Publishing Switzerland. Series in Advanced Microelectronics, – 2016, – vol. 53, 159 p.

ADAPTIVE PLANAR ANTENNAS ON LATTICES OF ROTATING DIELECTRIC RESONATORS

Trubin A. A.

*National Technical University of Ukraine
“Igor Sikorsky Kyiv Polytechnic Institute”
E-mail: atrubin@ukrpost.net*

АДАПТИВНІ ПЛАНАРНІ АНТЕННИ НА РЕШІТКАХ ОБЕРТОВАНИХ ДІЕЛЕКТРИЧНИХ РЕЗОНАТОРІВ

Досліджуються властивості планарних антен побудованих на решітках обертованих діелектричних резонаторів.

The use of rotating DR in various lattices significantly expands the possibilities of constructing a wide class of devices, antennas, channel switches, multiplexers, and other elements of microwave and optical communication systems [1-3]. The purpose of this report is to investigate antennas built on rotating DRs.

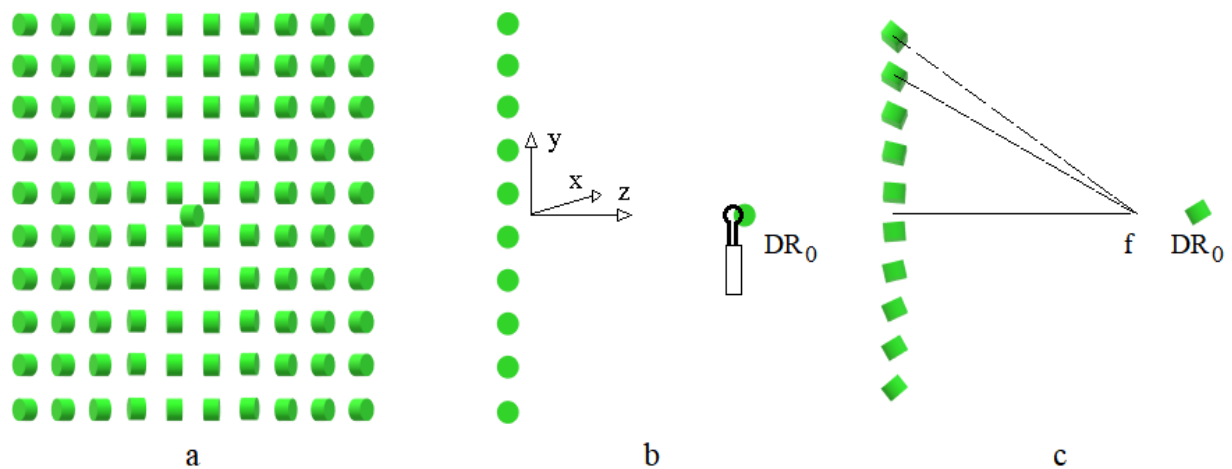


Fig. 1. Planar antenna image on Rotating Cylindrical Dielectric Resonators (a - d).

We investigated the square lattice with a relative distance between the centers $L_x = L_y = 1/4\lambda_0$ of the adjacent resonators (Fig. 1), where λ_0 - is the wavelength in open space. The dimensions of the DR corresponded to the condition of excitation of the main magnetic oscillations in them H_{101} . The dielectric constant of each DR was assumed to be equal $\epsilon_{1r} = 36$; $\text{tg}\delta = 10^{-3}$; relative sizes $\Delta = L/2r_0 = 0,44$ (Here r_0 - is the radius, L - is the height of the DR).

Active DR_0 was excited by a metal wire loop. Every DR had the ability to rotate about the y-axis (Fig. 1, a - c). In this case, the planes of the lattice rotated with the condition that a focus is formed on the z-axis at a distance f (Fig. 1, c). DR_0 also could rotate at an arbitrary angle relative to the y-axis. The distance between the active resonator did not coincide with the focal length f .

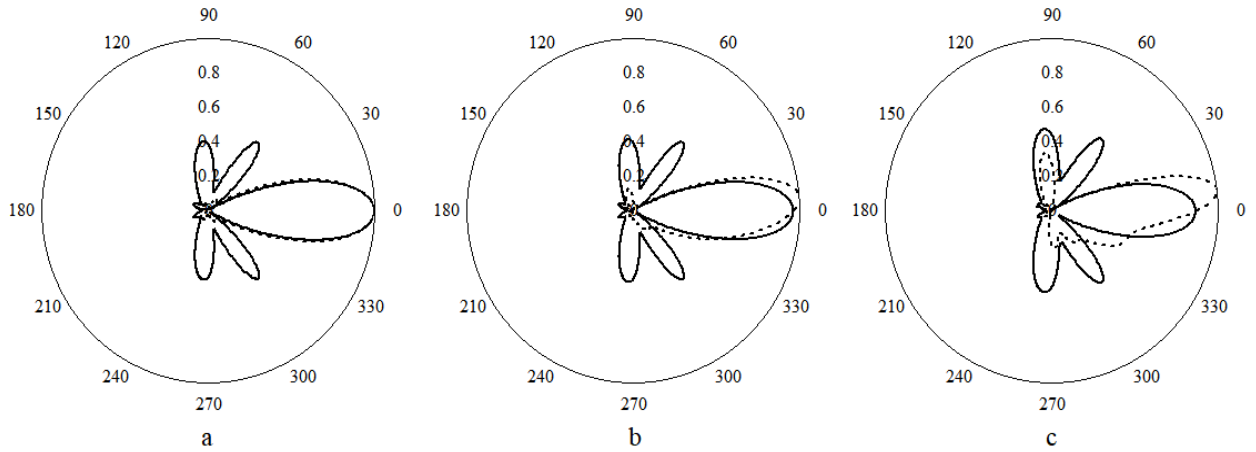


Fig. 2. Antenna pattern depending on the angle of active DR_0 rotation: $\varphi_0 = 0$ (a); $-0,1\pi$ (b); $-0,2\pi$ (c).

We have created a lattice model [4], in which the DR mutual coupling coefficients were calculated using formulas taken from [5]. The result of calculating the antenna beam for different orientations of the DRs is shown in Fig. 2.

Where φ_0 - is the angle between the axis of the DR_0 and the x-axis (Fig. 1, b). In the E-plane, the antenna pattern is shown as a solid line, and in the H-plane as a dashed line.

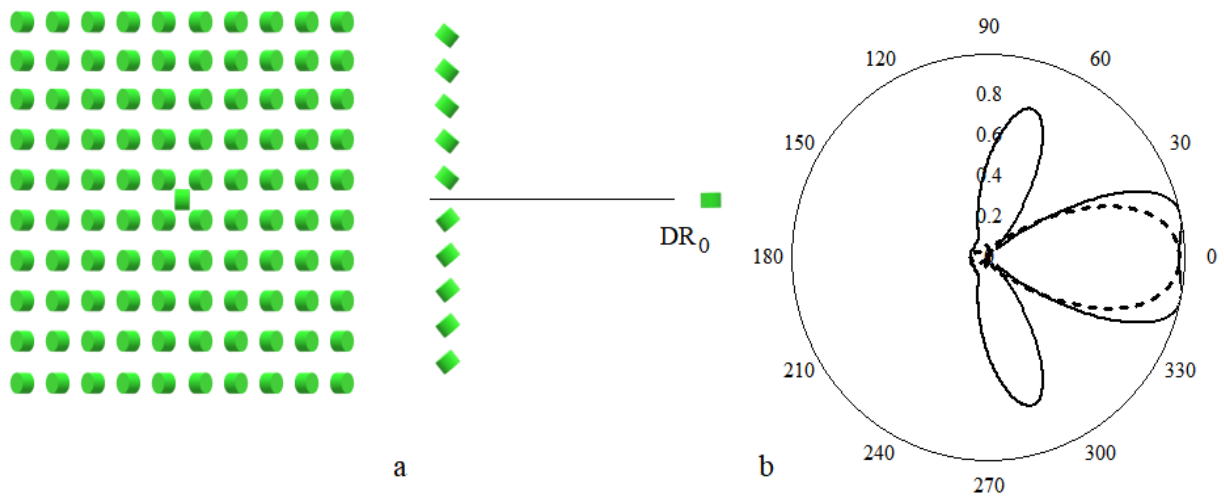


Fig. 3. Planar antenna with semi lattice identical rotation (a). Antenna pattern depending on the angle of the DR rotation: $\pm 1/6\pi$ (b).

Rotating half of the DR grating (Fig. 3, a) allows expanding the directional pattern in the direction of the main lobe (Fig. 3, b).

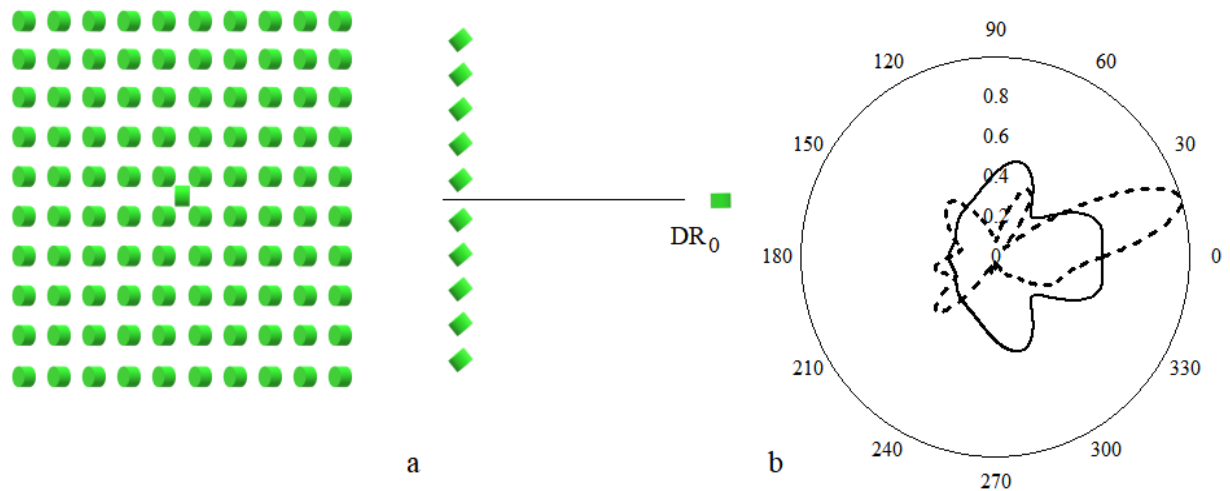


Fig. 4. Planar antenna on Dielectric Resonators with lattice identical rotation (a). Antenna pattern depending on the angle of lattice DR rotation: $1/3\pi$ (b).

The build an antenna array at the same rotation of the all DRs is shown in Fig. 4. In this case, a change in DR angle has a more noticeable effect on the radiation pattern (Fig. 4, b) rotation.

As follows from the results obtained, the synthesized antennas has good responsiveness of the direction of the main lobe at small angles of rotation of the resonators. The greatest change in the direction of the main lobe is achieved by rotation of all the resonators of the lattice. For small angles, rotation of only the active DR can be applied.

The above results can be used to design adaptive wireless access antennas in microwave, infrared, and optical wavelength communication systems.

References

1. N. Michishita, A. Lai, T. Ueda, T. Itoh. Tunable Dielectric Resonator-Based Left-Handed Leaky Wave Antenna, Proceedings of ISAP, 2007, Niigata, Japan, pp. 1466-1469.
2. P. Gutruf, C. Zou, W. Withayachumnankul, M. Bhaskaran, S. Sriram, C. Fumeaux. Mechanically Tunable Dielectric Resonator Metasurfaces at Visible Frequencies, *Acs nano*, 2016, 10, pp. 133-141.
3. D. Neshev, I. Aharonovich. Optical metasurfaces: new generation building blocks for multi-functional optics, *Light: Science & Applications*, 2018, No.7:58, pp. 1 - 5.
4. Trubin A.A. Lattices of Dielectric Resonators, Springer International Publishing Switzerland. Series in Advanced Microelectronics, – 2016, – vol. 53, 159 p.
5. Trubin A.A. Coupling coefficients of different cylindrical dielectric resonators in the open space, *Bulletin of NTUU "KPI" ser. Radiotechnique, Radioapparatus Building*, 2016. No. 66, pp.37-45.

Секція 3. Технології транспортних телекомунікаційних систем та мережні технології

UDC 004.051

OPTIMIZE OPTICAL DATA NETWORKS USING SDN TECHNOLOGIES

¹Saychenko I.O., ¹Kamarali R.V., ²Romanov M.O.

*¹National Technical University of Ukraine "Igor Sikorsky Kiev Polytechnic Institute", ²Kyiv College of Communication, Ukraine
E-mail: paramayson@gmail.com*

Оптимізація оптичних мереж передачі даних з використанням технології SDN

Контролер T-SDN (транспортні програми, визначені програмним забезпеченням) дає змогу автоматизувати значну частину мережевих операцій і, як результат, дозволяє оператору значно заощадити час - сотні годин, які інженери витрачають на налаштування мережі та надання послуги. За допомогою спрощення операцій по роботі з транспортною мережею та оптимальним використанням пропускної спроможності каналу виконується автоматична конфігурація мережі та спрощує роботу мережевим інженерам та зменшує витрати для кінцевого користувача. У рамках транспортного рівня кластеризація системи може бути відокремлена від способів прискорення прокладки шляху, а також оптимізації напруги на контрольному рівні низького рівня.

You will not surprise anyone with start-ups and developments in the field of software-defined networks (SDN) - the topic is widely studied by both large world corporations and open source communities.

T-SDN (transport software-defined networks) controller produced by NetCracker company has been deployed on the network of one of the European operators. The controller automated a significant part of network operations and, as a result, allowed the operator to significantly save time - hundreds of hours that engineers spent on setting up the network and providing the service [1].

The main idea of T-SDN, as well as in SDN for data centers, is the separation of the data plane and the control plane, which is implemented through the creation of a single control controller that interacts with network devices of a certain domain of the transport network. Above the controller is the application layer (SDN application layer), which communicates with the controller via a specific interface. Due to the fact that the controller knows everything about the structure of its domain, there are additional opportunities for improving the network. For some of them, solutions already exist in various protocols, but T-SDN can significantly improve existing approaches [2, 3].

So what does T-SDN (Figure 1.)offer:

- Simplification of operations with the transport network.

It is assumed that requesting a service from a provider will be as simple as placing an order in an online store. Once the order is placed, the controller will

automatically reconfigure all devices and allocate the necessary resources. Thus, the client will receive the necessary service in minutes.

- Optimal bandwidth utilization.

Optimizing the use of channel capacity (or, as they say, the optimal utilization of the channel) is not a new task. However, a complete solution for the dynamic distribution of client channels in the transport network still does not exist, and it is assumed that in the future the transport controller will take care of this task.

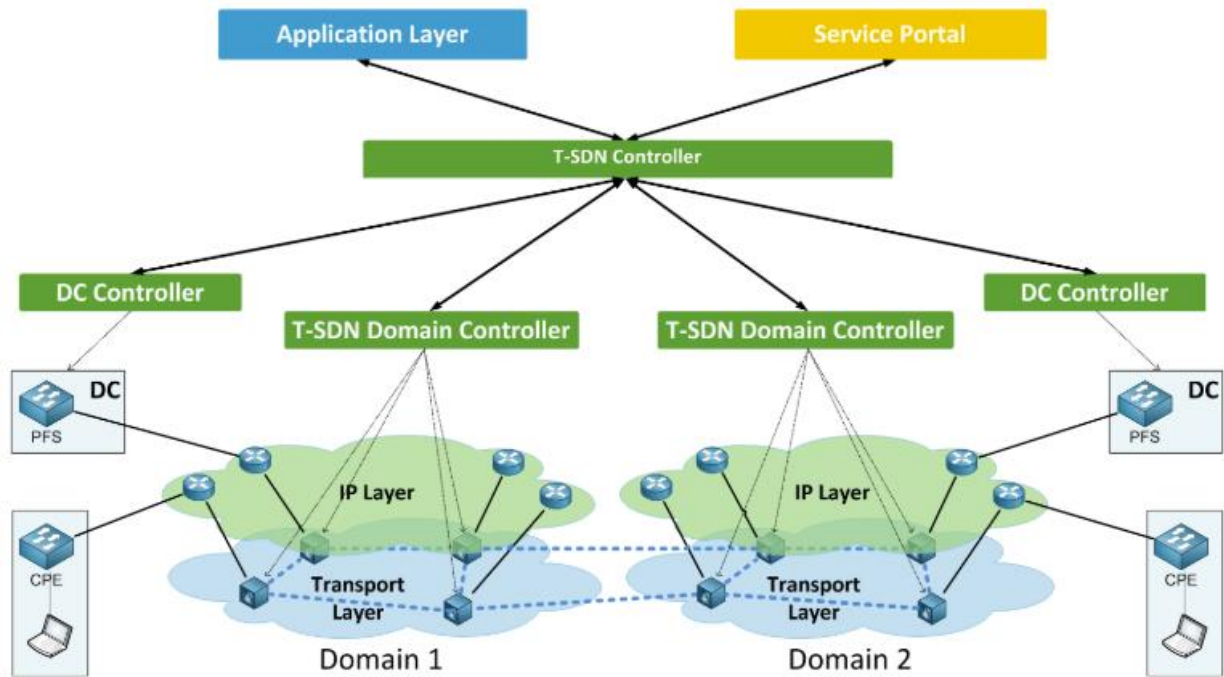


Figure 1. Multi-domain transport network architecture.

The successful launch of the pilot version enables the T-SDN controller developers to contribute to the development of Open Source projects such as ONOS and ODNOS, to participate in the standardization of new SDN technology in the Open Networking Foundation and in other organizations. The project is being developed in close cooperation with NEC, a manufacturer of modern network equipment. Thus, the controller's functionality is tested in the NetCracker network laboratory on the latest devices from NEC, and the development departments of NetCracker and NEC have the opportunity to closely collaborate and directly discuss technical issues. This interaction allows you to better understand the capabilities of vendors and work more efficiently with network devices. Significant development will have (and already are [4]) absolutely all the components - from low-level network interfaces Mediator (the Mediation) to the imaging and control applications. Controller Team T-SDN company NetCracker, which has many years of experience working with leading providers within OSS- and BSS- making sure initiated the development of this difficult but highly interesting region [1].

Requests for services "bandwidth on demand" are carried out by the Service

Orchestrator, which is architecturally related to the application level for the Controller.

Based on the data received from the underlying infrastructure, the controller can create multi-level virtual topologies that include all levels of existing transport networks: 1) L0 (WDM ROADM), 2) L1 (OTN), 3) L2 / L3 + (IP / MPLS).

All controller operation should be as close to real-time as possible. There is the concept of Active Real-Time.

First of all, the path calculation time is determined by the size of the topology formed on the basis of the network. However, technological specificity (for example, for DWDM) has significant weight. Based on the experience gained by the NetCracker team as a result of the implementation, we can say that calculating the path on one segment of the provider's network (controlled by the lower-level controller) takes less than 50 ms. The time taken by the top-level controller to calculate the path can vary significantly. This is due to the fact that it aggregates various network domains within itself. So, for example, the calculation of the path during load testing on a topology consisting of 10,000 elements took about 2 seconds [3].

Within the transport level of the system, clustering can be one of the ways to speed up the laying of the path, as well as optimizing the load on the lower level controllers.

It is also important to note that the time taken by the controller to calculate the path is negligible compared to the time that may be required to lay or re-route this path at the level of optical equipment.

Initially, the top-level controller is responsible for ensuring the optimal laying of the service according to the criteria obtained from the Service Orchestrator. Traffic optimization is performed both on the upper and lower level controllers. This process affects not only the main routes (Main), but also backup (Protection).

Controllers can monitor network parameters (such as bandwidth, traffic balancing and load of deployed VNFs) both independently and through third-party systems.

Reference

1. Deart Vladimir Yuryevich, Fatkhulin Timur Dzhalevich Analysis of transport software-configured networks (T-SDN) with a controlled optical level in order to obtain a model that allows us to assess the possibility of providing the service Bandwidth on Demand // T-Comm. 2018. No4. URL: <https://cyberleninka.ru/article/n/analiz-transportnyh-programmno-konfiguriruemyh-setey-t-sdn-s-upravlyaemym-opticheskim-urovnem-s-tselyu-polucheniya-modeli> (viewed 03.03.2020).
2. Huawei official website, T-SDN Overview <http://developer.huawei.com/en/ict/Products/SDN/Components/Forum/Banner/en/TSDNOOverview> (viewed 03.03.2020).
3. Deart V. Yu., Fatkhulin TD (2017). Analysis of current state of transport networks with the purpose of introducing software defined networks (SDN) technology. T-Comm, vol. II, no.6, r. 4-9
4. T8 official website, Catalog of DWDM systems "Volga", URL: http://t8.ru/wp-content/uploads/2018/05/Catalog-T8-Volga_rus.pdf (viewed 03.03.2020).

ПОБУДОВА МЕРЕЖІ SDN З ВИКОРИСТАННЯ ПЛАТФОРМИ SEBA

¹Кочура М.Ю., ²Романов М.О.

¹Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського,

²Київський коледж зв'язку

E-mail: ko4ura228@gmail.com, smartboobs1927@gmail.com

Popular SDNs using SEBA platform

Currently, the introduction of SDN technology is one of the most important areas of telecommunications development worldwide. This article is about building broadband access on SDNs using SEBA. The article defines the SEBA platform and its place in the structure of ONF projects. The system architecture, the list of elements, their purpose and functions are considered.

В даний час, одним із найважливіших напрямків розвитку телекомунікацій у всьому світі є впровадження технології SDN. Ця стаття стосується питань побудови широкопasmового доступу в мережах SDN за допомогою SEBA. В статті дається визначення платформи SEBA та її місце в структурі проєктів ONF. Розглядається архітектура системи, перелік елементів, їх призначення та функції.

Широкопasmовий доступ з підтримкою SDN (SEBA) - це зразок платформи, яка будується спільнотою ONF та CORD. SEBA - це легка платформа, заснована на варіанті R-CORD. Вона підтримує безліч технологій віртуалізованого доступу на межі мережі операторів. SEBA підтримує як житловий доступ так і бездротовий зворотний зв'язок і оптимізований таким чином, що трафік може проходити «швидкою доріжкою» прямо до магістралі, не вимагаючи обробки VNF на сервері [1].

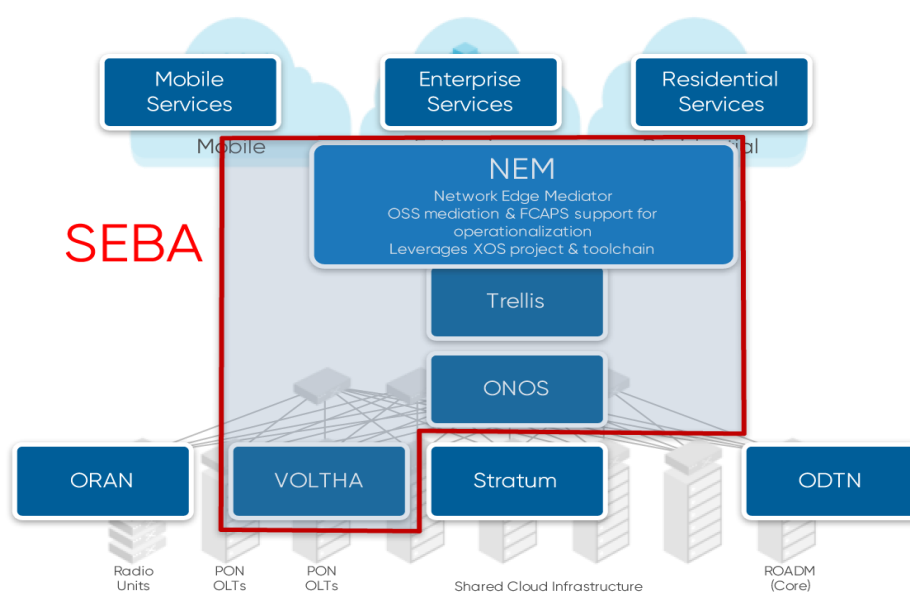


Рис. 1. Місце SEBA в структурі проєктів ONF.

Як показано на рис 1, SEBA є об'єднанням ряду проєктів ONF, таких як VOLTHA, ONOS і TRELIS. Вона забезпечує створення шаблону архітектури та розробки рішень для широкосмугового доступу [2].

SEBA повинна надавати інформацію про набір рішень для цих версій програмного забезпечення. SEBA - платформа на базі Kubernetes, де все програмне забезпечення управління розгортається як контейнери на обчислювальних вузлах, використовуючи оркестрацію Kubernetes, створюючи потім SEBA Pod (групу контейнерів).

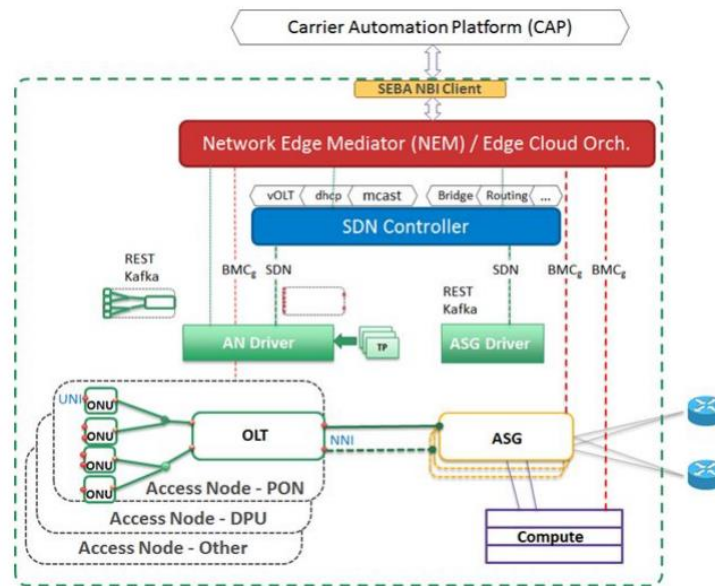


Рис. 2. Модульна архітектура платформи SEBA.

Як показано на рис. 2, SEBA складається з декількох програмних модулів високого рівня, включаючи:

- Медіатор Edge Network (NEM);
- Модуль управління SDN;
- Модуль керування програмами;
- Драйвер доступу до вузла (AN);
- Драйвер агрегації та обслуговування (ASG).

Архітектура SEBA вимагає дотримання деяких принципів та визначень:

1. Інфраструктурний шар не позначається, але він включає фізичні компоненти - вузли доступу, перемикачі агрегації та обчислення.

2. Сервісний шар визначає прив'язку компонентів до рівня інфраструктури для надання послуг.

3. Контролер SDN підтримує самостійність структури управління для кожного компонента інфраструктурного шару, що бере участь у наданні сервісу.

4. Модуль ASG підтримує агрегацію, перемикання та маршрутизацію площини даних, площини управління та трафік сигналізації в межах POD і підтримує можливості Service Edge.

5. Контролер управління платою (BMC) - це функціональне визначення та галузевий термін для інтерфейсу до функцій управління обладнанням.

У составі SEBA Pod є обладнання OLT та ONU, кероване VOLTHA, яке керує мережею PON, і контролер SDOS ONOS, який включає в себе пару API / додаток, які відкривають послуги, що надаються PON. Наприклад, OLT підключається до пари вимикачів ASG, якими також керуватиме контролер SDN. Потім обладнання комутаторів може підключатися до зовнішніх маршрутизаторів та / або BNG, до локальних комп'ютерів, тощо [3].

Однією з особливостей, що робить SEBA відмінною від R-CORD, є те, що трафік плати даних для абонента просто проходить через апаратне забезпечення та виходить в Інтернет. Це створює для абонентського трафіку "швидкий шлях" до Інтернет. Шлях даних залишається апаратним і виходить лише для обчислення вузлів, коли це необхідно, наприклад, коли для певних абонентів надаються сторонні послуги. Для порівняння, у R-CORD трафік, що надходить від резидентного абонента, проходить через апаратне забезпечення, але потім він переходить до обчислення вузлів через віртуальний комутатор, як OVS, та відвідує контейнер VSG (Virtual Subscriber Gateway), а потім повертається назад в апаратне забезпечення та в Інтернет [3, 4].

Таким чином, платформа SEBA надає можливість удосконалити мережі доступу, вирішити питання побудови відкритих інтерфейсів, керованих програмним забезпеченням сучасних систем у нових ключових областях, таких як багатогігабітні мережі з волоконним доступом.

Література

1. [Електронний ресурс] – Режим доступу до ресурсу: (<https://www.opennetworking.org/seba/>)
2. Романов О.І., Діденко І.В. Особливості взаємодії контролера і мережевих пристроїв в мережах SDN з використанням протоколу OPENFLOW. Матеріали одинадцятої МНТК «Проблеми телекомунікацій», Київ, 2017 р. С 142-145.
3. Романов О.І., Федюшина Д.М., Донг Т.Т. Аналіз принципів побудови фізичного та MAC рівнів у LI-FI – системах. Матеріали одинадцятої МНТК «Проблеми телекомунікацій», Київ, 2017 р. С 126-128.
4. SDN Enabled Broadband Access) [Електронний ресурс] – Режим доступу до ресурсу: (<https://www.opennetworking.org/wp-content/uploads/2019/04/ONF-Reference-Design-SEBA-032919.pdf>)

АНАЛІЗ ВРАЗЛИВОСТІ БЕЗДРОВОЇ МЕРЕЖІ WI-FI З НОВИМ ПРОТОКОЛОМ ЗАХИЩЕНОСТІ WPA3

Підпалий О.І., Романов О.І.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського,

E-mail: sashapidpalyi@gmail.com

Analysis of wireless vulnerability WI-FI with new WPA3 security protocol

To date, the issue of data confidentiality is one of the most important in the world. Most of the valuable information is contained on phones and laptops that are constantly connected to Wi-Fi. Therefore, the issue of wireless security is the highest priority to date[1,2]. The WPA2 security protocol has long been the best in this regard, but as time goes on, technology gets older and attackers become more creative and competent about hacking Wi-Fi. This is why the new WPA3 security protocol was created, with its new Wi-Fi security features.

На сьогоднішній день питання конфіденційності даних є одним із найважливіших в світі. Більшість цінної інформації містяться на телефонах і ноутбуках, які постійно підключені до Wi-Fi. Тому питання захищеності бездротової системи є найпріоритетнішим на сьогодні [1,2]. Протокол захищеності WPA2 довгий час являвся найкращим в цьому плані, але з часом технологія старіє, а зловмисники стають більш креативними і компетентними в питанні взлому Wi-Fi. Саме для цього було створено новий протокол захисту WPA3, зі своїми новими засобами захисту Wi-Fi.

До 2017 року WPA2 вважався одним із найбільш безпечних протоколів. Але у 2017 році в протоколі WPA2 була виявлена серйозна вразливість, що отримала назву KRACK (**K**ey **R**einstallation **A**ttack), яка дає можливість зловмиснику атакувати 4-х стороннє рукостискання протоколу WPA2, тобто ініціювання WPA2-з'єднання. Це рукостискання відбувається кожного разу, коли клієнт хоче приєднатися до захищеної Wi-Fi мережі WPA2, щоб підтвердити, що клієнт і точка доступу мають правильні облікові дані, тобто пароль Wi-Fi, перед тим, як клієнт приєднається до мережі. Під час того ж 4-х стороннього рукостискання встановлюється свіжий ключ шифрування, який використовується для шифрування подальшого трафіку. Маніпулюючи цим рукостисканням, зловмисник може обманути жертву перевстановивши вже використаний ключ шифрування, тоді як ключ повинен бути встановлений і використаний лише один раз. Перевстановлення ключа шифрування змушує скинути два лічильника (відомі як "nonces"), використовувані протоколом шифрування, і це дозволяє атакувати на протокол, наприклад, повторення, розшифрування або підробка пакетів. Потенційний зловмисник, який перебуває у фізичній близькості від захищеної мережі Wi-Fi і здійснює цю атаку, відому як "людина-в-

середині".[3] Зловмисник може по суті перехоплювати та розшифровувати інтернет-трафік без володіння обліковими даними захищеної мережі Wi-Fi (тому зміна пароля Wi-Fi не допоможе). Ключова атака переустановки проілюстрована на спрощеному рис. 1.



Рис. 1. Ключова атака переустановки (KRACK).

Цей факт, поряд з усіма раніше відомими недоліками WPA2, підштовхнув Wi-Fi Alliance до розробки - WPA3. Вже в липні 2018 року Wi-Fi Alliance оповістив про початок сертифікації пристроїв, що підтримують WPA3 (Wi-Fi Protected Access 3) - найбільшого оновлення захисту за минулі 14 років. WPA3 став офіційним із запуском у червні програми сертифікації Wi-Fi Alliance для WPA3-Personal, що забезпечує більш індивідуальне шифрування, та WPA3-Enterprise, що збільшує криптографічну силу для мереж, що передають конфіденційну інформацію[4].

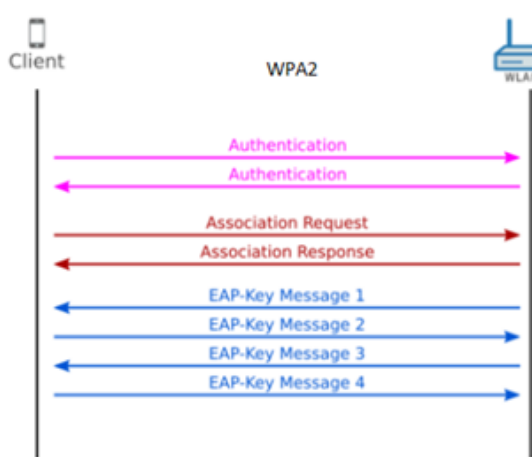


Рис. 2. Схема підключення WPA2.

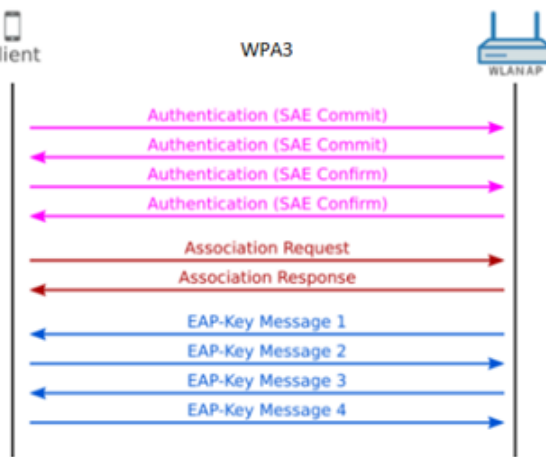


Рис. 3. Схема підключення WPA3.

У WPA2 завжди гострою проблемою залишалося використання слабких паролів. Якщо користувачі ставлять легкий пароль на бездротову мережу, то його запросто можна було підібрати через автоматизовані атаки з використанням словників, таких як Dictionary і Brute-Force. WPA2 не мав варіантів для усунення такої проблеми. Якраз тому в WPA3 був вжитий новий механізм автентифікації SAE (Simultaneous Authentication of Equals), який замінює використовуваний в WPA2 метод PSK (Pre-Shared Key). SAE

перекладається як "одночасна автентифікація рівних", і згідно з цим алгоритмом автентифікація пристроїв проводиться одночасно і на рівних правах. SAE надає допоміжне покращення безпеки, якого не було в PSK: пряму секретність [forward secrecy] [5].



Рис. 4. Повідомлення автентифікації WPA3.

```
> Frame 924: 188 bytes on wire (1504 bits), 188 bytes captured (1504 bits)
> Radiotap Header v0, Length 56
> 802.11 radio information
> IEEE 802.11 Authentication, Flags: .....C
v IEEE 802.11 wireless LAN
  v Fixed parameters (104 bytes)
    Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3)
    Authentication SEQ: 0x0001
    Status code: Successful (0x0000)
    SAE Message Type: Commit (1)
    Group Id: 256-bit random ECP group (19)
    Scalar: 37a6fb24eb390c40f276bc2dd259aabd525859dd5a25faaf...
    Finite Field Element: 67bda0b066db0c8b8b0ccf1934647df09a8055d461ec161c46...
```

Рис. 5. Повідомлення SAE 1.

```
> Frame 928: 188 bytes on wire (1504 bits), 188 bytes captured (1504 bits)
> Radiotap Header v0, Length 56
> 802.11 radio information
> IEEE 802.11 Authentication, Flags: .....C
v IEEE 802.11 wireless LAN
  v Fixed parameters (104 bytes)
    Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3)
    Authentication SEQ: 0x0001
    Status code: Successful (0x0000)
    SAE Message Type: Commit (1)
    Group Id: 256-bit random ECP group (19)
    Scalar: 60962e7d30a9e7b4cf825333a7f1bcb836bde18194a124bc...
    Finite Field Element: 371b8cac4f268af96755b08a106d8cf3c9accea93579d2d4...
```

Рис. 6. Повідомлення SAE 2.

```
> Frame 933: 124 bytes on wire (992 bits), 124 bytes captured (992 bits)
> Radiotap Header v0, Length 56
> 802.11 radio information
> IEEE 802.11 Authentication, Flags: .....C
v IEEE 802.11 wireless LAN
  v Fixed parameters (40 bytes)
    Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3)
    Authentication SEQ: 0x0002
    Status code: Successful (0x0000)
    SAE Message Type: Confirm (2)
    Send-Confirm: 1
    Confirm: 9bd771c8a5d75f154101922d13cf78a6a70dd724c4606b30...
```

Рис. 7. Повідомлення SAE 3.

```
> Frame 935: 124 bytes on wire (992 bits), 124 bytes captured (992 bits)
> Radiotap Header v0, Length 56
> 802.11 radio information
> IEEE 802.11 Authentication, Flags: .....C
v IEEE 802.11 wireless LAN
  v Fixed parameters (40 bytes)
    Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3)
    Authentication SEQ: 0x0002
    Status code: Successful (0x0000)
    SAE Message Type: Confirm (2)
    Send-Confirm: 0
    Confirm: 4532733f7b02350c35fde405fe41b3faf461975a5ab0322...
```

Рис. 8. Повідомлення SAE 4.

Повідомлення SAE 1 - Користувач надсилає повідомлення AP в AP з його ідентифікатором групи, скаляром та новою точкою на Еліптичній кривій (інформація про Кінцевий елемент поля).

Повідомлення SAE 2 - AP відправляє своє повідомлення "Здійснювати" на пристрій користувача зі своєю скалярною та ECC точкою.

Повідомлення SAE 3 - Користувач надсилає своє повідомлення підтвердження до AP з маркером підтвердження.

Повідомлення SAE 4 - AP відповідає своїм підтвердженням та маркером, і тепер асоціація може статися, якщо був встановлений захищений канал.

З використанням SAE при кожному новому з'єднанні встановлюється новий шифр пароля, тому навіть якщо розбійник в якийсь момент і проникне в мережу, він зможе вкрати тільки пароль від даних, переданих після цього моменту[6].

Виходячи з загального положення і спираючись на сукупність всіх вище перелічених фактів можна сказати, що на зміну, вже менш безпечного протоколу WPA2 приходить сучасний і більш ефективніший протокол WPA3, який має безліч переваг, таких як: більш безпечне рукостискання, заміна налаштувань на захист Wi-Fi (WPS), несанкціоноване шифрування і більші розміри ключів сеансу. Однак усі ці переваги WPA3 реалізуються лише тоді, коли всі пристрої будуть підтримувати цей протокол і розгортання цієї мережі почнеться лише тоді, коли на ринку з'явиться більше пристроїв кінцевих користувачів WPA3.

Література

1. Романов О.І., Осокін М.Г. Аналіз рівня безпеки сигналізації SS7. Матеріали 12-ої МНТК «Проблеми телекомунікацій», Київ, 2018 р. С 131-134.
2. Письменний І.С., Романов А.О. Мережа підприємства с програмним забезпеченням ASTERISK PBX на основі PLC, Київ, 2018 р. С 119-122.
3. Огляд вразливості Wi-Fi WPA2 [Електронний ресурс] – Режим доступу до ресурсу: <https://www.enisa.europa.eu/publications/info-notes/an-overview-of-the-wi-fi-wpa2-vulnerability>.
4. WPA2 vs. WPA3. [Електронний ресурс] – Режим доступу до ресурсу: https://www.diffen.com/difference/WPA2_vs_WPA3.
5. WPA3 - Підвищення безпеки вашої WLAN [Електронний ресурс] – Режим доступу до ресурсу: <https://wlan1nde.wordpress.com/2018/09/14/wpa3-improving-your-wlan-security//>
6. Покращення безпеки Wi-Fi: WPA3-Personal(SAE) [Електронний ресурс] – Режим доступу до ресурсу: <https://wificoops.com/2019/07/28/wi-fi-security-enhancements-part-1-wpa3-personal-sae//>

МЕТОД ЗМЕНШЕННЯ ЧАСУ ДОСТАВКИ ПОВІДОМЛЕНЬ В IP МЕРЕЖІ ЗА РАХУНОК МОДИФІКАЦІЇ ПРОТОКОЛУ UDP

Маньківський В.Б., Педько А.Д.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: v.b.mankivskiy@gmail.com , andreypedko99@gmail.com

A method of reducing the delivery time of messages on an ip network by modifying the UDP protocol

This article has compared the most common transport layer protocols and their disadvantages. A method for modifying the UDP protocol for networks is described, and the parameters that need to be modified to achieve higher data rates are identified. In addition, an easily scalable network for future UDP testing with modified parameters has been built.

У роботі порівняно найпоширеніші протоколи транспортного рівня і вказані їх недоліки. Описано метод модифікації протоколу UDP для невеликих приватних мереж та визначено параметри котрі необхідно змінити для досягнення більшої швидкості передачі даних. А також побудована легко масштабуєма мережа для майбутнього тестування протоколу UDP зі зміненими параметрами.

Основою передачі повідомлень в архітектурі TCP/IP лежить в зоні відповідальності транспортного рівня, а саме протоколу. Створити протокол транспортного рівня, який би зміг задовольнити потреби потенційних користувачів як в швидкості, так і в надійності є досить складною задачею. З одного боку, потрібна високошвидкісна мережа для з'єднання мережевих пристроїв в межах будівлі, а з іншого - надійні комунікаційні мережі між комп'ютерами, рознесеними на сотні кілометрів. Для вирішення цієї проблеми були створені протоколи, котрі могли б задовольняти ті чи інші вимоги користувачів, але в рамках своєї реалізації й при цьому неодноразово.

Областю дослідження цієї роботи являється транспортний рівень моделі OSI, оскільки саме протоколи цього рівня відповідають за передачу даних по будь-якій мережі. Оскільки, транспортний рівень - це перший рівень для створення сеансу зв'язку, який зустрічає дані додатки і починає процедуру по їх підготовці до передачі.

В даний час існує два основних протоколу транспортного рівня – це TCP та UDP. Десять років тому всі були абсолютно впевнені, що UDP - це протокол про негарантовану доставку [1]. Обидва протоколи TCP і UDP – функціонують на транспортному рівні та вирішують завдання доставки повідомлень.

На відміну від TCP, UDP – здатний досягти значно вищі швидкості передачі, оскільки в ньому використовується самий механізм встановлення з'єднання, який орієнтований на передачу. Доставка UDP не гарантує доставку даних, датаграма має шанс загубитися, і можуть бути отримані дві копії одного і того ж повідомлення. Якщо при використанні UDP потрібна надійна передача даних, її слід реалізувати в протоколі вищого рівня [2]. Таким чином, використовуючи протокол UDP, можна знизити навантаження мережі.

Перед тим як починати модифікацію протоколу, необхідно визначити параметри, які можуть вплинути на основні параметри передачі, а також визначити величину їх впливу[3]. В якості практичного стенду було побудовано мережу з наступними параметрами, яка зображена на Рис.1. В якості клієнтів використано ОС Ubuntu 16.04, мережеві пристрої з образами від компанії Cisco в середовищі моделювання GNS 3.0, протокол маршрутизації - RIPv2.

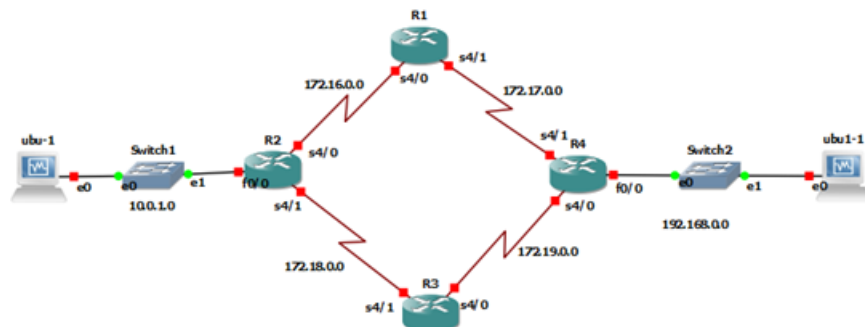


Рис. 1. Проект мережі для тестування протоколу UDP.

Отже, приступимо до вибору параметрів котрі необхідно модифікувати для прискорення роботи мережі на прикладі протоколу TCP. Вибір параметрів залежить від сфери використання даного протоколу. Якщо необхідно забезпечити передачу відео в FullHD, то швидкості передачі на прийомному тракті в 400Мбіт/с, параметр RTT буде приблизно 250 мс.

Так як TCP це протокол з використанням підтвердження, то всі дані, які не отримали підтвердження про доставку, зберігаються в буфері. Якщо буфер на відправку обмежений 128 Кб, то ці 128 Кб менші ніж за RTT, ми відправити не зможемо [4]. Таким чином, на прийомному кінці від 400 Мбіт/с залишиться 4 Мбіт/с. Таким чином можна зробити висновок, що для того щоб ефективно обмінюватися даними на великі відстані необхідно змінити розмір буфера.

Простим рішенням є автоматична настройка розміру буфера. Зараз це використовується на багатьох клієнтських додатках. При цьому за одну передачу може бути відправлено кількість пакетів, яка рівна розміру буфера. При успішній передачі, збільшується розмір буфера (величина розміру визначається стандартом TCP), передача даних прискорюється, розмір буфера зростає. При такому підході з'являється проблема пов'язана з тим, що процес зменшення буфера використовує складніший алгоритм. Оскільки, буфер досить великий і весь заповнений, потрібно чекати, поки всі дані будуть відправлені.

При використанні модифікованого UDP протоколу, то є доступ до буферу. TCP в таких ситуаціях відповідно до стандарту додає дані в кінець [5,6]; змінити цей алгоритм неможливо. При модифікації UDP протоколу можна поміщати дані, наприклад, вперед, відразу ж за On-the-fly пакетами. При отриманні від клієнтського обладнання cancel, то можна очистити буфер.

Інший параметр, який розглядається для модифікації є packet pacing. Цей параметр задає темп відправки пакетів. Оскільки, чим довше відбувається відправка пакетів, тим більша вірогідність втрати пакетів. Якщо пакети надсилати з певним інтервалом часу, то втрата пакетів зменшиться. Гіпотеза дослідження: якщо задати рівномірний темп відправки пакетів, то швидше за все, імовірність переповнення буферів стане нижче.

Наступний параметр MTU – розмір даних котрі можна переправити по мережі. Відправляючи пакети з сервера на клієнт, наприклад, розміром 1500 біт. Якщо на шляху зустрічається маршрутизатор, котрий не підтримує цей розмір MTU, то маршрутизатор фрагментує ці пакети. Отже, важливо правильно визначити величину MTU, оскільки при фрагментації при втраті одного пакета, буде відкинуті й інші, що може значно підвищує час доставки.

Таким чином, виконавши модифікацію параметрів описаних вище, можна підвищити швидкість роботи мережі та знизити втрату пакетів. Остаточне порівняння модифікованого протоколу UDP та звичайного TCP:

1. В протоколі TCP навіть правильна зміна буферу може викликати проблеми з мережею, а в UDP можна змінювати буфер коли завгодно.
2. При використанні протоколу TCP можна використовувати тільки існуючі типи Congestion control. При використанні UDP, можна обрати будь-який.
3. В TCP важко додати новий Congestion control оскільки доведеться модифікувати acknowledgement. Це можна зробити лише на сервері.
4. TCP має проблеми з мультиплексуванням даних при втрачених пакетах, а отже протокол HTTP2.0 не дає великого приросту в швидкості.
5. Випадки, коли ви можете отримати встановлення з'єднання за 0-RTT в TCP вкрай рідкісні, близько 5%, і близько 97% - модифікованого протоколу UDP.

Література

1. Kumar S. and S. Rai, "Survey on Transport Layer Protocols: TCP & UDP", International Journal of Computer Applications, 2012. 46(7): p. 20-25.
3. Singh, S.K., R. Duvvuru, and J.P. Singh, "TCP and UDP-based performance evaluation of proactive", Journal of Information and Communication Technology, 2015.: p. 632-644.
4. Skulysh M., Romanov O. The structure of a mobile provider network with network functions virtualization. // Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, 2018 14th International Conference on. IEEE, 2018 - Pages: 1032 - 1034
4. Romanov O., Hordashnyk Y., Dong T.. Method for calculating the energy loss of a light signal in a telecommunication Li-Fi system // Proceedings of the 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo).
5. Romanov O, Mankivskyi V. Optimal traffic distribution based on the sectoral model of loading network elements, IEEE Problems of Infocommunications. Science and Technology Trans. Multimedia, 2019, pp. 210–219.
6. Nor, S.A., R. Alubady, and W.A. Kamil, Simulated performance of TCP, SCTP, DCCP and UDP protocols over 4G network. Procedia computer science, 2017. 111: p. 2-7.
7. Romanov O., Nesterenko M., Veres L. IMS: Model and calculation method of telecommunication network's capacity // Proceedings of the 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo).

КОНЦЕПЦІЯ ГРАНИЧНИХ ОБИЧИСЛИНЬ В МЕРЕЖІ МОБІЛЬНОГО ОПЕРАТОРА

Маньківський В.Б., Педько А.Д.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: v.b.mankivskiy@gmail.com , andreypedko99@gmail.com

Concept of edge computing in mobile operator network

Today, there are two concepts of mobile edge computing (MEC): the installation of physical equipment and cloud solutions. Blockchain, as the main technology of the now popular digital currency Bitcoin, has become a promising decentralized data management base. Although blockchain is widely used in many applications, its use in mobile services is still limited. Because, it consumes considerable resources in terms of CPU time and energy. To make blockchain programs easier on future mobile systems, edge computing is the solution. The paper proposes the concept of boundary computing for mobile blockchains.

На сьогоднішній день існують дві концепції граничних обчислень на підприємстві: установка фізичного обладнання та хмарні рішення. Блокчейн, як основна технологія нині популярної цифрової валюти Bitcoin, стала перспективною децентралізованою базою управління даними. Незважаючи на те, що блокчейн широко застосовується у багатьох програмах, його застосування в мобільних послугах все ще обмежене. Оскільки, витрачаються значні ресурси з точки зору часу та енергії процесора. Щоб полегшити програмам блокчейн у майбутніх мобільних системах крайові обчислення виступають рішенням. В роботі запропоновано концепцію крайових обчислень для мобільних блокчейнів.

Ключовою концепцією для гарантування цілісності та достовірності даних у блокчейн є обчислювальний процес, визначений як майнінг [1]. Щоб додати новий блок даних до поточного блокчейна, користувачеві блокчейна (miner) потрібно вирішити обчислювальний доказ роботи (PoW), щоб отримати хеш- значення, яке пов'язує попередній блок з поточним блоком. Багаторазовий протокол консенсусу дає нагороду успішному miner як стимул для вирішення PoW (Рис.1). Однак, завдяки необхідному внеску в обчислення PoW, вузли з обмеженими ресурсами, такі як Internet of Things (IoT) та мобільні пристрої не можуть безпосередньо брати участь у процесі видобутку, що представляє серйозну проблему в блокчейн-додатках для мобільних служб.

Мобільна крайова обчислювальна технологія (MEC – mobile edge computing) [2] була введена для використання доступної обчислювальної потужності в мобільних середовищах (Рис.1). Локальні центри обробки даних та сервери розміщуються постачальником послуг на «межі» мобільних мереж, таких як базові станції мереж радіодоступу. MEC - ключова технологія для задоволення суворих вимог із низькою затримкою мереж покоління 5G [3].

Мобільні пристрої можуть отримати доступ до крайових серверів, щоб підвищити їх обчислювальну здатність (наприклад, обробка даних зондування IoT). Завдяки цій функції крайові обчислення стають перспективним рішенням для мобільних блокчейн-додатків.

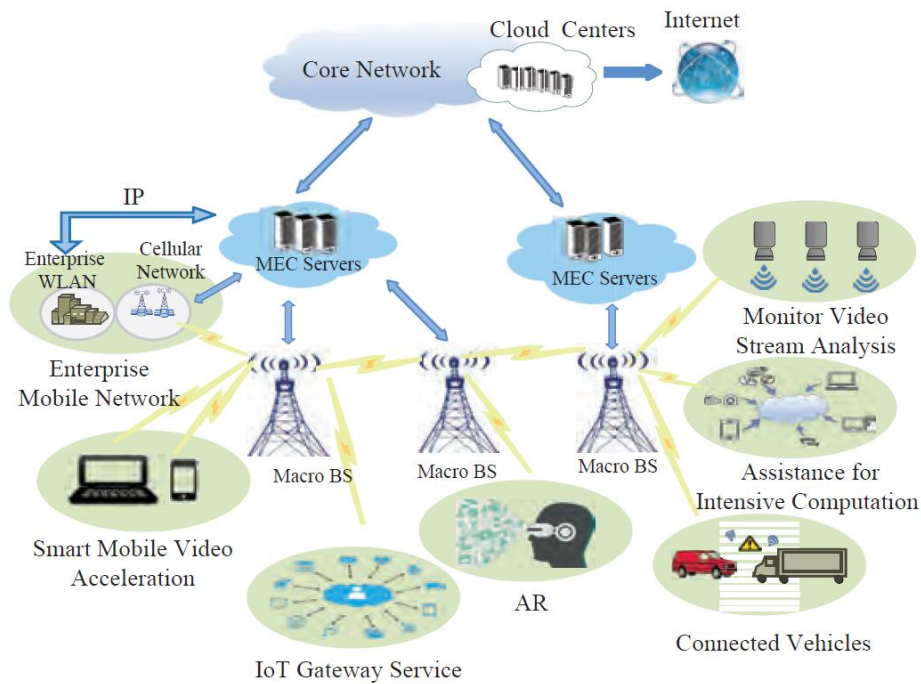


Рис. 1. Архітектура граничних обчислень в мережі мобільного Оператора.

Наприклад, у [4] автори запропонували механізм ціноутворення для стимулювання спільної комунікації між мобільними терміналами, що може значно зменшити як зв'язок, так і відключення акумулятора. У роботі розглянуто мобільну блокчейн-мережу з підтримкою крайових обчислень, де IoT або мобільні пристрої можуть отримувати доступ та використовувати ресурси або обчислювальні послуги від кращого постачальника обчислювальних послуг [5] для підтримки своїх додатків блокчейну.

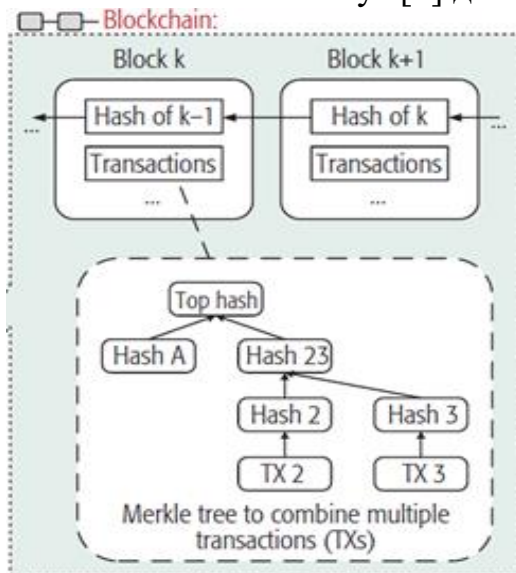


Рис. 2. Структура блокчейн

Блокчейн Architecture. Основна ідея блокчейн - це ланцюгова структура даних, яка також називається ланцюжком блоків або блокчейн. Кожен блок даних містить перевірені історичні дані або транзакції. Організація даних у Блокчейн: На Рис. 2 представлена схема структури блокчейна. Кожен блок в блокчейн зазвичай містить дві частини: дані транзакцій та хеш-значення. Дані про транзакцію записують користувачі або системи блокчейн (наприклад, мобільні пристрої). Значення хешу використовуються для зберігання кодової або захищеної інформації.

Пошук консенсусу. Основна задача при використанні блокчейн – це необхідність того, щоб більшість користувачів змогли довести, що блок дійсний, він буде доданий до поточного блокчейна. Це процес консенсусу.

Поширений консенсус: Блокчейн може запропонувати більше, ніж криптовалюта для транзакцій та даних у недовірливих розподілених

мережах. Консенсус - це механізм забезпечення довіри до мережі, який означає, що користувачі в мережі зазвичай досягають згоди. Розгортання консенсусу корисно для розподілених обчислювальних систем з незалежними користувачами, наприклад мобільних мереж [6,8].

Розв'язуючи PoW, слід обчислити значення, яке робить значення хеша заголовка нижче, ніж задана "ціль складності". Підтвердження та забезпечення цілісності та дійсності угод виконуються набором miner. У багатьох системах блокчейн (наприклад, Bitcoin) miner, який успішно виконує блок, отримує винагороду за видобуток, коли добутий блок успішно додається до блокчейн. Консенсус гарантує безпеку та надійність систем блокчейн [7,9]. У мережі блокчейн, де майнінг коштує дорого, зловмисникам потрібно контролювати понад 51% усієї обчислювальної потужності в мережі, щоб маніпулювати.

Mobile Edge Computing (MEC) Services. Останнім часом блокчейн знайшов багато застосувань у різних мережах та розподілених системах; одна з них – IoT [4]. Однак пристрої IoT малопотужні та географічно розподілені. Обмежений обчислювальний ресурс та енергозабезпечення пристроїв IoT стають основними бар'єрами. Натомість мобільні пристрої можуть постачати обчислювальні та комунікаційні ресурси для мобільного блокчейна.

MEC [4,6] дозволяє постачальникам послуг розгортати хмарні обчислювальні послуги на «краю» мобільного Інтернету, як показано на Рис. 1. Наприклад, базові станції, обладнані невеликим центром обробки даних або набором серверів у мережах радіодоступу, здатні приймати завантажені завдання з сусідніх мобільних пристроїв та пристроїв IoT [6]. Взаємодія між крайовими постачальниками послуг обчислювальної техніки та користувачами IoT можна моделювати як ринкову діяльність, де постачальники продають такі ресурси, як дані та обчислювальна потужність, отримуючи дохід від користувачів IoT. На практиці реалізована аналогічна концепція, наприклад, Microsoft надає блокчейн як послугу (BaaS) на хмарній платформі Azure. Незважаючи на всі хмарні послуги блокчейн, економічні моделі транзакцій блокчейн в крайових обчислювальних системах недостатньо вивчені.

Концепт MEC для Mobile Блокчейн. Крайові обчислення для мобільних блокчейнів було реалізовано на наступному прототипу. У мережі мобільної мережі блокчейн вузли (наприклад, мобільні пристрої) повинні виконувати майнінг на крайовому обчислювальному сервері. Прототип використовує робочу станцію, як крайовий обчислювальний сервер, а мобільні пристрої як постачальники консенсусу. Вузли виконують роль miner, встановлюючи клієнтський додаток для мобільних блокчейнів. Робота виконана на прикладі криптовалюти Bitcoin, яка й досі не втрачає своєї популярності та є однією з найбільш часто використовуваних блокчейн-платформ. Мобільні пристрої підключаються до крайового обчислювального сервера через мережевий концентратор за допомогою клієнтської програми мобільного блокчейна. Основні етапи видобутку для експерименту:

1. Створено 1000 блоків за допомогою сервера Node.js.

2. На мобільних пристроях ініційовано видобуток блоків.
3. Гірники запитують обчислювальну послугу з сервера.
4. Приймають рішення про видобуток блоку.
5. Фіксуємо попит на обчислювальні послуги.
6. Змінюємо попит, в залежності від значення попиту іншого miner.
7. Розмір блоку однаковий на всіх запитах.

Було досліджено два випадки: з п'ятьма та дев'яти miner. У випадку з п'ятьма miner спочатку зафіксовано попит на обчислювальні послуги (процент використання процесора) у 40 та 60 та зміна попиту іншого miner.

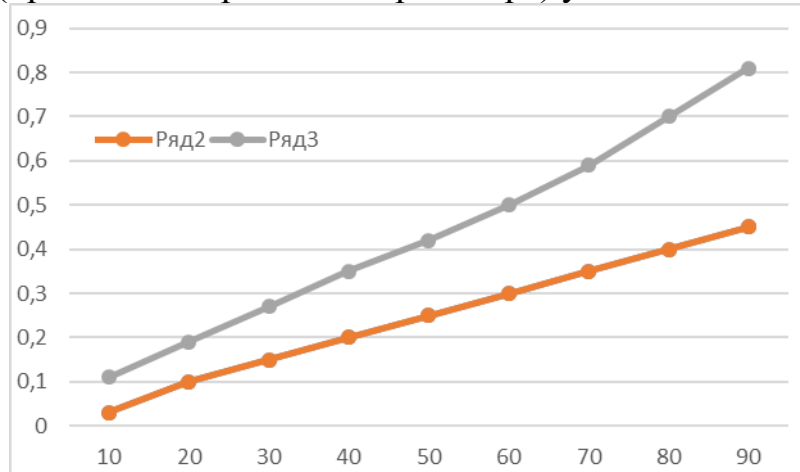


Рис. 3. Результати зміни попиту
(ряд 2 – 5-ть miner, ряд 3 – 9-ть miner).

У випадку з дев'яти miner ми фіксуємо попит трьох miner на 40, 50 та 60 і змінюємо попит іншого miner. Кількість транзакцій у кожному видобутому блоці становить 10. Результати експериментів показані на Рис. 3, на якому ми бачимо, що в міру збільшення попиту на обчислювальні послуги

в ймовірність того, що miner успішно дістає блок, вище.

Ми також порівнюємо експериментальні результати з аналітичними результатами, отриманими в [5,8]. Очевидно, що аналітичні та експериментальні результати добре відповідають.

Література

1. R. Pass and E. Shi, "FruitChains: A Fair Blockchain," PODC'17 Proc. ACM Symp. Principles of Distributed Computing, Washington, DC, July 25–27, 2017, pp. 315–24.
2. S. Wang, et al., "A Survey on Mobile Edge Networks: Convergence of Computing, Caching and Communications," IEEE Access, vol. 5, 2017, pp. 6757–79.
3. Romanov O, Mankivskiy V. Optimal traffic distribution based on the sectoral model of loading network elements, IEEE Problems of Infocommunications. Science and Technology Trans. Multimedia, 2019, pp. 210–219.
4. Y. Guo, L. Duan, and R. Zhang, "Optimal Pricing and Load Sharing for Energy Saving with Cooperative Communications," IEEE Trans. Wireless Commun., vol. 15, Sept.2016, pp. 951–64.
5. Z. Xiong, et al., "When Mobile Blockchain Meets Edge Computing", IEEE Access, vol. 5, August,2018, pp. 33 - 39.
6. O.I. Romanov, M.M. Nesterenko, L.A. Veres. IMS: Model and calculation method of telecommunication network's capacity // Proceedings of the 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo) 11-15 Sept. 2017 Year, Odessa, Ukraine. - IEEE Conference Publications.
7. K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, May 2016, pp. 2292–2303.
8. Mariia Skulysh, Romanov Oleksandr. The structure of a mobile provider network with network functions virtualization. // Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, 2018 14th International Conference on. IEEE, 2018 - pp.: 1032 – 1034.

ПОБУДОВА КОНТРОЛЕРА МЕРЕЖІ SDN З ВИКОРИСТАННЯ ХМАРНИХ РЕСУРСІВ

Романов О.І., Шихов М.С.

Інститут телекомунікаційних систем КІП ім. Ігоря Сікорського, Україна

E-mail: a_i_romanov@ukr.net, maxshkv@gmail.com

Architecture of SDN controller for use in cloud resources

The basic trends among cloud resources providers are summarized. The results of simulation of cloud computing using different SDN implementations are presented.

Програмно-конфігуровані мережі (SDN) - це концепція, яка дає можливість операторам мережі та центрам обробки даних гнучко керувати мережевими обладнаннями, використовуючи програмне забезпечення, що працює на зовнішніх серверах.

Основна вимога програмного забезпечення для хмарних мереж полягає в тому, щоб мережеве обладнання та програмне забезпечення були відносно відкритими та сумісними, щоб програмні платформи можна було легко встановити або перемістити через стандартне обладнання, що відповідає галузям. Це дає можливість переносу та програмування мережевої інфраструктури.

На рис.1 представлений найпростіший приклад взаємодії мережевого пристрою SDN (Network Device) і контролера SDN (Controller). Мережевий пристрій SDN і контролер SDN взаємодіють один з одним через спеціальний канал SDN (SDN channel). Цей канал може бути як відкритим, так і захищеним. Роботою каналу керує процесор мережевого пристрою SDN за допомогою функціонального блоку, що називається Менеджер каналу SDN (Channel Manager).

Основними елементами мережевого пристрою є процесор і таблиця маршрутизації. Мережевий пристрій SDN приймає потоки трафіку від клієнтських пристроїв, або інших мережевих пристроїв і передає їх згідно змісту власної таблиці маршрутизації.

Потік трафіку є потоком з одного або декількох пакетів, що переносять дані з джерела в пункт призначення. Мережевий пристрій SDN здатний ідентифікувати та направити пакети конкретному потоку даних на основі адреси джерела, адреси призначення та іншої інформації в заголовку пакетів. Кожен запис в таблиці маршрутизації відповідає певному потоку трафіку.

Слід зазначити, що канал SDN використовується для передачі тільки керуючої інформації. Це може бути, наприклад:

- заявка від МП-SDN до контролера на пошук маршруту для пакета, який не має необхідних даних в таблиці маршрутизації;
- відповідь контролера SDN про внесення необхідних змін до таблиці маршрутизації при появі нових потоків і зміни структури мережі.

Зазвичай передача інформації по каналу SDN ведеться з використанням протоколу OpenFlow.

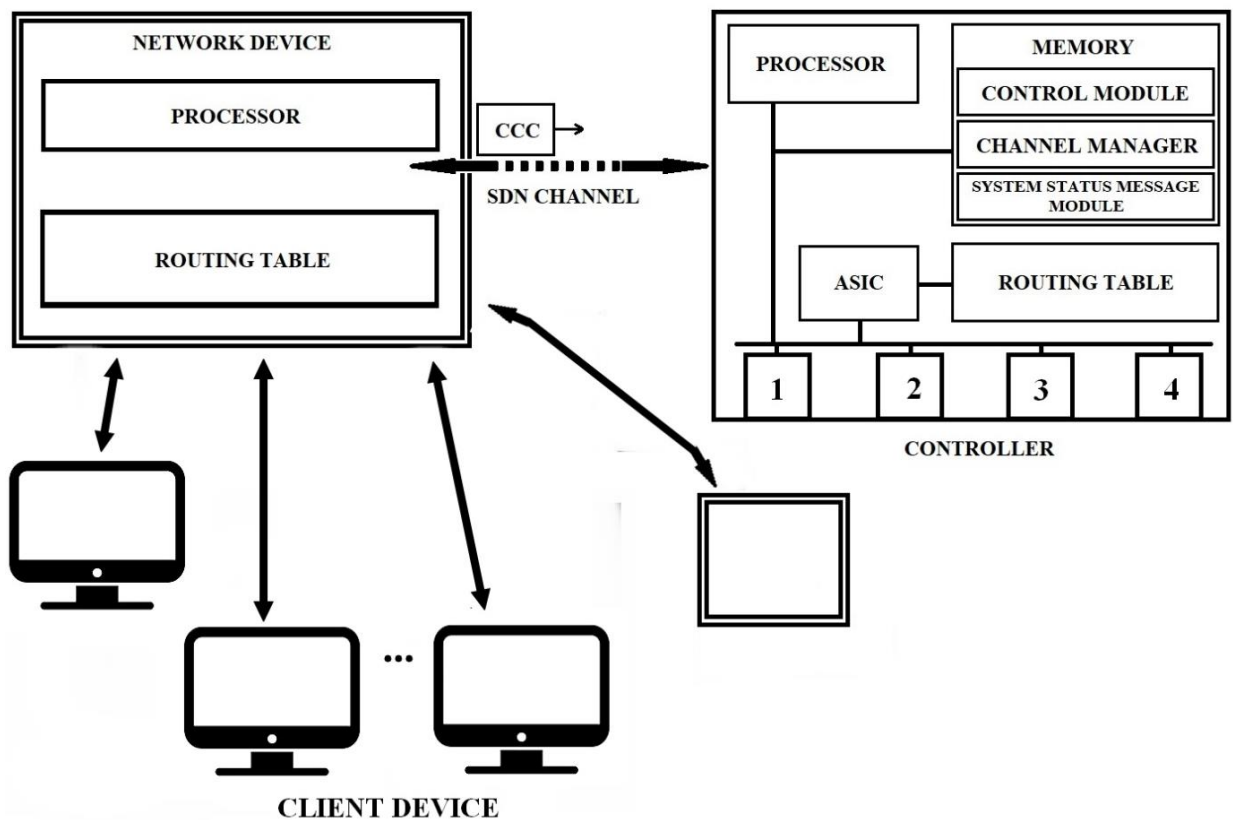


Рис. 1. Найпростіший приклад взаємодії в мережі SDN.

Прийняття SDN може покращити керованість мережею, масштабованість та динамічність у центрі обробки даних підприємств. Основні та крайові вузли з підтримкою SDN з належним SDN контролером і мережевим додатком можуть розглядатися як новий механізм об'єднання хмар.

Об'єднання, що базується на SDN, сприятиме збільшенню кількості мереж від багатьох постачальників між дата-центрами провайдерів і приватних підприємств, допомагаючи корпоративним клієнтам вибирати кращих постачальників у своєму класі, уникаючи при цьому залежності від конкретних постачальників обладнання; вибрати належну технологію доступу з широкого спектру (наприклад, DWDM, PON тощо); отримати доступ до динамічної пропускної здатності під спеціальні задачі, своєчасна міграція та обробка навантаження між даними дата-центрів; та усунути тягар недостатньо використаних, затратних приватних орендованих ліній великої ємності. Послуги з пропускною здатністю на вимогу, що підтримуються SDN, надають автоматизоване та розумне надання послуг, кероване логікою оркестрування хмарних послуг та вимогами замовника.

Хмарні мережі та віртуалізація серверів повинні бути за необхідності масштабованими та оркестрованими. В ідеальній ситуації фізична мережа забезпечить транспорт, а гіпервізори нададуть послугу віртуалізації і віртуальні мережі будуть побудовані поверх транспортної мережі. Традиційний підхід - це реалізувати віртуальні сегменти за допомогою VLAN, які обмежені 4096 сегментами (VLAN) і, отже, не є дійсно здатними

до масштабування. Є кілька пропозицій, які пропонують використовувати IEEE 802.1ad для подолання цього обмеження.

Одним з них є Nicira NVP. Відображення MAC-to-IP завантажується у Open vSwitch за допомогою централізованого OpenFlow контролера. Цей контролер усуває потребу в будь-якій надлишковості, як це потрібно в VXLAN. Віртуальні комутатори, які використовуються у такому підході використовують протокол OpenFlow, що означає, що віртуальними комутаторами може керувати зовнішній контролер OpenFlow (наприклад, NOX). Ці Open vSwitch'і використовують точкові GRE тунелі, які, на жаль не сумісні з OpenFlow. Ці тунелі мають бути передбачені за допомогою інших механізмів, оскільки у OpenFlow немає повідомлення про надання тунелю. Відкритий протокол управління базами даних vSwitch (OVSDB) використовується для побудови повних сітчастих тунелів GRE між хостами. Цей підхід масштабується краще, ніж VXLAN, оскільки у фізичній мережі немає стану, який би підтримувався. Крім того, для зупинки перевантаження L2 можна використовувати проксі ARP. Це вимагає, щоб контролери OpenFlow і OVSDB працювали паралельно, щоб автоматично забезпечувати тунелі GRE.

Таблиця 1. Порівняння реалізації віртуальних мереж.

Technology	Bridging	All hosts flooding	vNet flooding	VLAN 4K limit	VM MAC visible	State kept in network
VLANs	+	+	+	+	+	+
VM-aware networking	+	-	+	+	+	+
vCDNI	+	+	+	-	-	MAC of hypervisors
VXLAN	-	Only to some hosts	+	-	-	Multicast groups
Nicira NVP	-	-	Some	-	-	-

Таким чином в роботі проведено аналіз процесу взаємодії контролера і мережевого пристрою в мережі SDN для використання хмарних ресурсів. VLAN, VM-свідома мережа, vCDNI, VXLAN та Nicira NVP - це технології надання віртуальних мереж у хмарній інфраструктурі. Nicira NVP, який використовує MAC для інкапсуляції IP та зовнішньої площини управління OpenFlow, забезпечує ефективне рішення для реалізації віртуальної мережі.

Література

1. <https://www.sdxcentral.com/networking/sdn/definitions/what-is-the-software-driven-cloud-networking/>
2. <https://patents.google.com/patent/WO2014192005A1/en>
3. Azodolmolky, Siamak & Wieder, Philipp & Yahyapour, Ramin. (2013). SDN-based Cloud Computing Networking (Invited). ICTON 2013. 10.1109/ICTON.2013.6602678.

БАГАТОВУЗЛОВА МЕРЕЖА SDN З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ LI-FI

¹Піталова М.Д., ²Мікляєв Г.О.

¹*Інститут телекомунікаційних систем КІП ім. Ігоря Сікорського*

²*Дійсний член МАН України*

E-mail: mkidalovaa@gmail.com, glibmiklaiv@gmail.com

Multinodular NETWORK TECHNOLOGIES SDN WITH LI-FI

The paper discusses a multi-node SDN network using Li-Fi technology. It is shown that the transition to this type of network can improve throughput and quality of service.

В роботі розглядається багато вузлова мережа SDN з використанням технології Li-Fi. Показано, що перехід до такого типу мереж дозволяє підвищити пропускну спроможність і якість обслуговування.

На сьогодні одна з найбільш поширених технологій безпроводового доступу є технологія Wi-Fi. Кожен з нас застосовує її для підключення комп'ютерів, мобільних телефонів, планшетів та інших пристроїв до Інтернету. Також Wi-Fi широко використовують у громадських місцях, таких як метро, гіпермаркети, стадіони, торговельно-розважальні центри аеропорти, майдани, в офісах компаній і фірм. Але користувачів стає все більше, зростають вимоги до пропускну спроможності систем і разом із тим збільшують радіочастотні завади. Як показує прогноз, наданий компанією CISCO, і попереджує Федеральна комісія радіозв'язку США, Wi-Fi підходить до межі своїх можливостей з пропускну здатності. Крім того, є обмеження на використання радіохвиль в літаках, лікарнях та інших місцях.

Тому, в якості одного із можливих напрямків подальшого розвитку систем безпроводового доступу, групою вчених з Единбурзького університету під керівництвом професора Гаральда Хааса запропонована технологія Li-Fi [1]. Li-Fi – це безпроводова оптична система зв'язку, в якій для передавання даних замість радіохвиль використовують світло. Різна амплітуда і швидкість мерехтіння світла дає змогу передавати дані. Інтенсивність мерехтіння дуже висока, тому людське око його не помічає. Технологія Li-Fi відносно нова. Тому всі системи на базі технології працюють поки ще в експериментальних умовах [2, 3]. Однак останнім часом, на базі технології Li-Fi пропонують абсолютно новий підхід до побудови систем безпроводового доступу щодо швидкості передавання даних, гнучкості та комфортності експлуатації і починають створювати зразки, які можливо використовувати на практиці.

На відміну від Wi-Fi під час використання технології Li-Fi використовуємо електромагнітний спектр між довжинами хвиль від 380 до 780 нанометрів. Крім того, це не ліцензований діапазон електромагнітного спектру, і тому його використання не потребує сплати за ліцензію, як це роблять для дозволу на використання радіодіапазону. На рис.1 зображено електромагнітний спектр різних видів сигналів. Як ми можемо бачити,

потенційна пропускна здатність діапазону видимого світла в 1000 разів вища ніж у радіодіапазоні [4]. Весь спектр між довжинами хвиль від 380 до 780 нанометрів може бути використаний для Visible Light Communication (VLC) На рис. 1 показано знаходження діапазону частини електромагнітного спектру видимого світла VLC.

Основна ідея VLC, який використовує Li-Fi, полягає у додаванні інформаційних даних до змін інтенсивності світла та виявлення змін на стороні приймача. Це називають методом прямого виявлення, модульованого інтенсивністю intensity modulated direct detected (IM/DD)^[9]. Використовувана частота модуляції зазвичай набагато вища, ніж може виявити людське око, і тому це не спричинює помітного мерехтіння в освітленні.

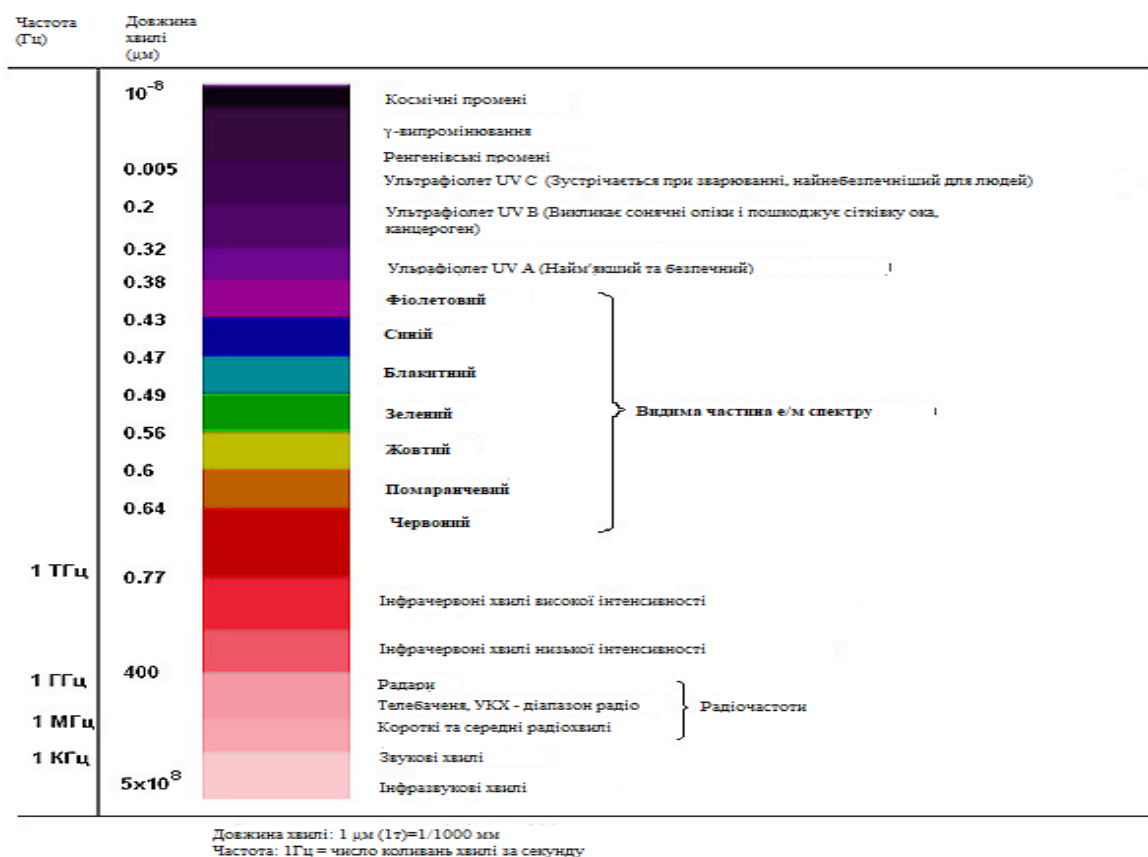


Рис. 1. Електромагнітний спектр різних сигналів.

VLC-зв'язок має ряд переваг. Основні з них це:

1. Смуга частот ширша в 1000 разів у порівнянні з радіо спектром [3].
2. Для впровадження технології Li-Fi можливе використання вже побудованої мережі освітлення приміщення. Це скорочує витрати на побудову мережі передавання даних.
3. Безпека для здоров'я і екологічна безпека.
4. Можливість використання Li-Fi там, де додаткове використання радіохвиль обмежено (літак та інше).
5. Використання неліцензованого спектру [5]. Тобто не потрібно сплачувати додатково за ліцензію.

Більшість існуючих випробувальних лабораторій для видимого світла

орієнтовані на реалізацію системи «точка-точка». Однак вже розроблені пропозиції до побудови систем видимого світла, які підтримують N вузлів [6]. На рис.2 представлено ієрархічна архітектура з трьома рівнями: хостом управління мережею, хостом управління SDR, апаратними засобами і інтерфейсами VLC. На верхньому (першому) рівні ієрархічної архітектури знаходиться вузол управління мережею. Вихід цього рівня являє собою набір оптимальних змінних, які потім будуть відправлені на кожен з керуючих хостів SDR. На другому рівні програмований стек протоколів (PPS) встановлюється на кожному з керуючих хостів SDR. З оптимальними змінними, отриманими від хоста управління мережею буде скомпільований стек протоколів PPS для генерації операційного коду для управління апаратними засобами VLC і зовнішніми інтерфейсами третього рівня. Нарешті, кожне апаратне і зовнішнє обладнання VLC (тобто USRP) отримує вибірки основної смуги частот від свого керуючого хоста через інтерфейс Gigabit Ethernet (GigE), а потім відправляє їх по радіоканалу з параметрами передачі, які зазначені в командах управління від SDR хостів.

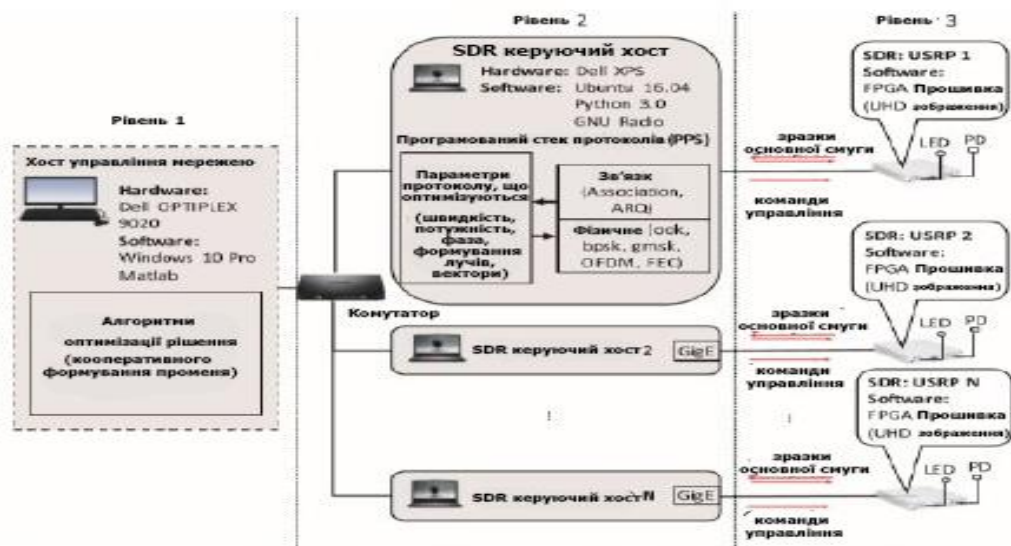


Рис. 2. Структурна схема програмованої системи мережі видимого світла.

Розглянемо призначення елементів системи:

1. Хост управління мережею - це настільний комп'ютер який має набір програм для вирішення завдань управління елементами мережі.
2. SDR керуючий хост - це програмований стек протоколів (PPS), який встановлюється на кожному з керівників хостів SDR. PPS може бути розробленим на програмному забезпеченні Python поверх GNU Radio. Це дозволяє забезпечити плавний контроль USRP. Наприклад, розроблений в роботі PPS [6] охоплює PHY і канальний рівні і може бути легко розширений до верхніх рівнів у майбутньому. Як показано на рис.3, архітектура вузлів на основі PPS дозволяє здійснити перевірку ефективності мережі у видимому світлі. На фізичному рівні може підтримуватися широкий набір схем модуляції, включаючи, включення-виключення (OOK), гаусову маніпуляцію

з мінімальним зрушенням (GMSK), двійкову фазову маніпуляцію (BPSK). Програмовані параметри на цьому рівні включають схеми модуляції і потужність передачі.

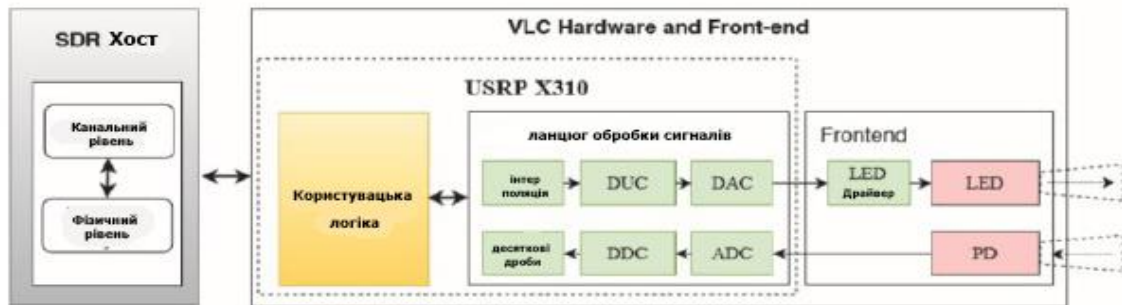


Рис. 3. Архітектура програмного забезпечення вузла видимого світла.

3. VLC Hardware і Front-end може бути реалізованим на материнській платі USRP X310 і має чотири широкосмугових слота для дочірніх плат.

Технологія VLC все ще перебуває на початковому етапі, і необхідні значні зусилля, поки можна буде використовувати весь потенціал для практичних застосувань. Проте, очікується, що ряд світлодіодних застосувань буде готовий через кілька років у багатьох секторах: від супутників до військових призначень, від лікарень (де слід уникати електромагнітних завад) до літаків, від освітлення до автомобілів.

Література

1. C. Chen, M. Ijaz, D. Tsonev, and H. Haas, "Analysis of downlink transmission in DCO-OFDM-based optical attocell networks," in Proc. of IEEE Global Communications Conference (GLOBECOM), Austin, TX, Dec 2014.
2. Y. Wang, X. Huang, L. Tao, J. Shi, and N. Chi, "4.5-Gb/s RGB-LED based WDM Visible Light Communication System Employing CAP Modulation and RLS based Adaptive Equalization," Optics Express, vol. 23, no. 10, pp. 13 626–13 633, May 2015
3. O.I. Romanov, Y. S. Hordashnyk, and T. T. Dong, "Method for calculating the energy loss of a light signal in a telecommunication Li-Fi system", International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), IEEE Conference Publications, Pages: 1-7, 2017;
4. Романов О.І., Федюшина Д.М., Донг Т.Т. Використання технології VLC для побудови мереж LI-FI та принцип її практичної реалізації. Матеріали 12-ої МНТК «Проблеми телекомунікацій», Київ, 2018 р. С 92-94.
5. Романов А.И., Федюшина Д.М., Донг Т.Т. Принцип построения беспроводной сети LI-FI и пути практической реализации // Матеріали 18 МНТК «Вимірювальна та обчислювальна техніка в технологічних процесах», Одеса, 2018 р., С 223-225.
6. Nan Cen, Neil Dave, Emre Can Demirel, Zhangyu Guan. LiBeam: Throughput-Optimal Cooperative Beamforming for Indoor Visible Light Networks May 2019.

ВИКОРИСТАННЯ ПРЕДМЕТНО-ОРІЄНТОВАНОЇ МОВИ ПРОГРАМУВАННЯ P4 ДЛЯ ПОБУДОВИ IMS

Полуденний О. М., Романов О. І.

Інститут телекомунікаційних систем КІП ім. Ігоря Сікорського, Україна

E-mail: alexpoludenniy@gmail.com

Use of P4 subject-oriented programming language to build IMS.

The relevance of the IMS concept for the construction of LTE mobile networks is analyzed. The stages of development of functional separation, abstraction of IMS - SDN are investigated. A variant of using P4 programming language in SDN networks is considered.

Технологія IMS дозволяє використовувати нові послуги зв'язку в мережах фіксованого та мобільного зв'язку і повністю забезпечує їх взаємодію з зовнішніми мережами, дозволяючи скоротити витрати операторів на будівництво інфраструктури.

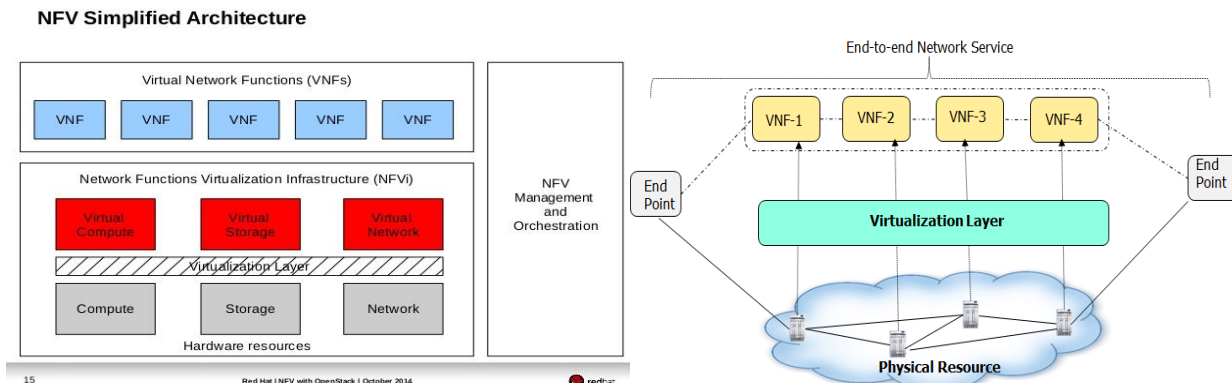
IMS дає можливість скоротити час установки з'єднання в мережі LTE в 6 разів до 1-2 секунд, передавати голос з високою якістю (HD-voice), вивести на новий рівень якості та доступності контентні послуги, а також дозволить абонентам, чий смартфон підтримує VoLTE, одночасно говорити по телефону і користуватися високошвидкісним мобільним інтернетом. Голосові виклики, ініційовані в мережі LTE, здійснюються в LTE мережі по IP на базі IMS-платформи (VoLTE).

У разі втрати LTE покриття голосовий виклик перенаправляється в 2G / 3G мережу комутації каналів (CS-voice). Для цього необхідна активація функціоналу Single Radio Voice Call Continuity. Застосування технології SRVCC дозволяє скоротити час встановлення голосового з'єднання в середньому до 1-ої секунди. Більш того, технологія дозволяє поліпшити якість голосового сервісу на 10-15%, ніж у мережі 2G / 3G.

Окрім голосового зв'язку по мережах передачі даних IMS дає можливість робити дзвінки по мережах Wi Fi (VoWiFi) та фіксованого інтернету (Voice over Broadband), передавати по мережах LTE відеосигнал (ViLTE), а також реалізовувати технологію RCS - стандарт, що дає можливість операторам запускати власні інтернет-месенджери.

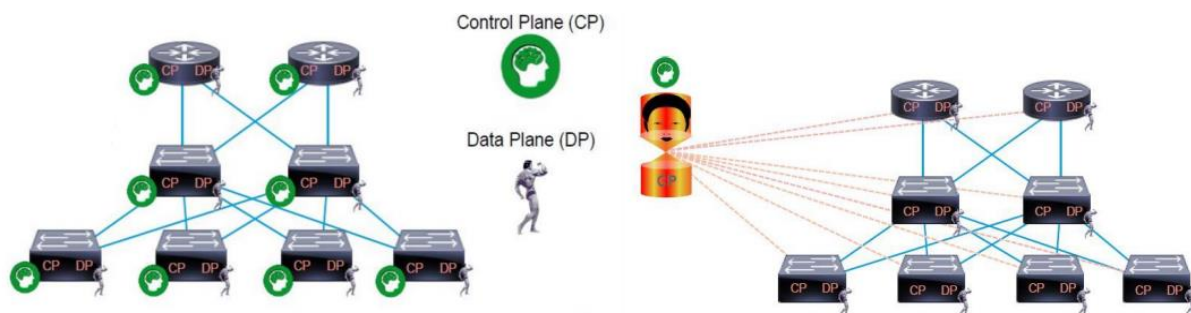
Підсистема мультимедійних послуг IP IMS (IP Multimedia Subsystem) наступний етап функціонального поділу, абстрагування, коли функції мережі відокремлюються від обладнання. У IMS всі різноманітні мережеві функції (CSCF, PCRF, MGSF, AGCF та ін.) - не обов'язково повинні були розташовуватися в одній стійці обладнання. Один функціональний блок міг знаходитися в різних одиницях обладнання та навіть в різних місцях розташування. Логічним кроком був наступний - а навіщо проектувати якісь спеціалізовані сервери для галузі телекомунікацій, а може краще використовувати стандартні сервери з ІТ і корпоративних мереж? Підвищення рівня надійності і потужності стандартного комерційного обладнання серверів для ІТ - COTS (Commercial Off The Shelf) дозволило вирішити цю задачу. Став можливий перехід до повної віртуалізації мережевих функцій. IMS - це, свого роду, предтеча архітектури віртуалізації мережевих функцій NFV, незважаючи на те, що їх архітектури сильно розрізняються.

Можна сказати, що NFV - це реалізація концепції IMS на стандартному комерційному IT-обладнанні, COTS. Різниця в тому, що в NFV функції реалізуються в програмному вигляді на стандартному серверному обладнанні в дата-центрах, а IMS - на спеціалізованому телеком-обладнанні. У NFV не має функціональних блоків IMS - всіляких CSCF, PCRF тощо. Там все було розроблено заново. Але концептуально - це продовження IMS.



SDN - це трохи окремо, і з'явилося це до NFV. NFV можна вважати одним з основних випадків використання SDN у системах постачальників послуг. Якщо говорити про абстрагування концепції NGN - IMS - SDN / NFV, то можна сказати, що:

- NFV - це відділення (абстрагування) функцій від обладнання.
- SDN - це відділення (абстрагування) управління від виконання, поділ Control Plane і Data Plane, якщо користуватися термінологією IP-маршрутизації.



Навіщо це взагалі треба? Навіщо розносити функціонал по різних рівнях?

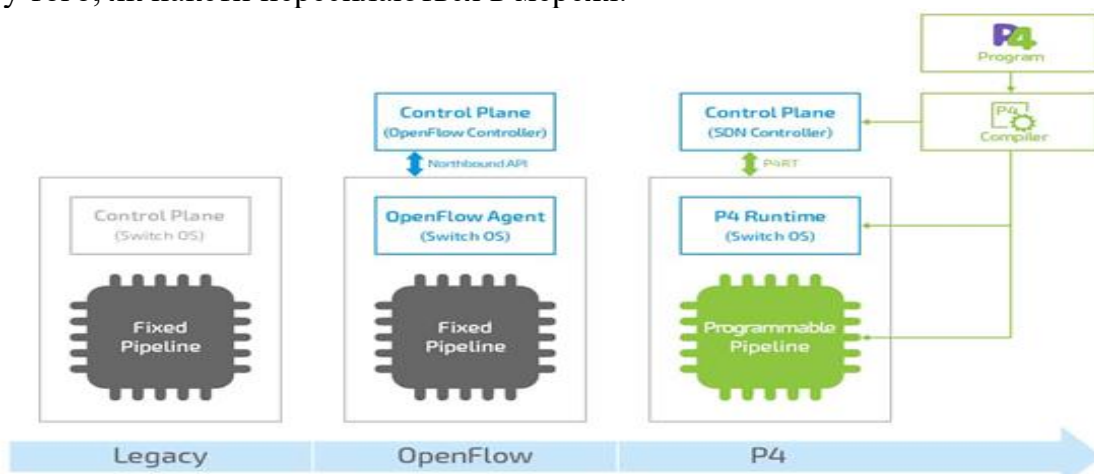
- По-перше, для того, щоб швидше ідентифікувати проблему в системі, і правильно визначити зону відповідальності.
- По-друге, щоб оперативніше вводити новий функціонал в мережу.
- По-третє, щоб спростити архітектуру протоколів, їх розуміння і освоєння інженерно-технічним персоналом.

Однією з ключових проблем, які намагається вирішити SDN-спільнота - є скорочення часу на впровадження нових протоколів і розширення їхнього функціоналу.

«SDN перетворив мережеву індустрію, а P4 виводить SDN на новий рівень, забезпечуючи програмованість в області маршрутизації», - сказав Гуру Парулкар, виконавчий директор Open Networking Foundation.

P4 - це мова програмування, призначена для програмування правил маршрутизації пакетів. На відміну від мов програмування загального призначення, таких як C або Python, P4 - це предметно-орієнтована мова з рядом конструкцій, оптимізованих для мережевої маршрутизації.

Мета: створити просту у використанні мову програмування, яку розробник програмного забезпечення зможе вивчити за день, і використовувати для точного опису того, як пакети пересилаються в мережі.



З самого початку P4 розроблявся як незалежний від цілі (тобто програма, написана на P4, могла бути скомпільована без змін для виконання на різних цілях, таких як ASIC, FPGA, CPU, NPU і GPU). Також P4 - протокольно незалежна мова, яка може описувати існуючі стандартні протоколи або використовуватися для вказівки нових настроюваних режимів адресації, може використовуватися як для програмованих, так і для пристроїв з фіксованою функцією. Наприклад: використовується для точного запису поведінки конвеєра комутатора в API-інтерфейсів інтерфейсу абстракції комутатора (SAI), використовуваних ОС комутатора з відкритим вихідним кодом SONiC. P4 використовується в проекті ONF Stratum для опису поведінки комутації через безліч стаціонарних і програмованих пристроїв.

Опис поведінки комутатора і мережевих адаптерів вперше дозволяє створити точну виконувану модель всієї мережі перед розгортанням. Великі хмарні провайдери можуть повністю тестувати і налагоджувати мережу за допомогою програмного забезпечення, що значно скорочує час і витрати на тестування взаємодії в лабораторії, не вимагаючи дорогого устаткування.

Використовуючи P4, постачальники мережевого обладнання можуть розраховувати на загальну базову поведінку маршрутизації у всіх продуктах, що дозволяє повторно використовувати інфраструктуру тестування, спрощує розробку програмного забезпечення для управління і, в кінцевому підсумку, гарантує сумісність.

Література

1. Телекомунікаційні та інформаційні мережі : Підручник [для вищих навчальних закладів] / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. – К.: САММІТ-Книга, 2010. – 708 с.: іл.
2. OpenFlow Table Type Patterns Version No. 1.0 15 August 2014.
3. <https://itechinfo.ru/content/voice-over-lte-volte>.
4. <http://lib.tssonline.ru/articles2/fix-corp/problems-razvitiya-oss-sistem-pri-migratsii-setey-ngn-ims-v-napravlenii-sdn-nfv>.
5. <https://shalaginov.com/2019/05/08/5773/>
6. <https://dou.ua/lenta/articles/p4-as-future-of-sdn/>
7. <https://habr.com/ru/company/fgts/blog/460439/>
8. <https://plvision.eu/rd-lab/blog/sdn/p4-programming-future-sdn>.

МОДЕЛЬ ДОСЛІДЖЕННЯ СИГНАЛІВ ОПТИЧНОГО ТРАКТУ З ВИКОРИСТАННЯМ SDR ТРАНСІВЕРА ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ GNURADIO

Літвінов Є.А., Романов О.І.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: litvinov_yevhenii@ukr.net

Optical path signal research model using an SDR transceiver and GNURadio software

The current trend in wireless communications with an ever-increasing demand for higher bandwidth and ubiquitous coverage is creating a high demand for the use of the radio frequency spectrum. This direction requires alternative ways to look for additional communication options in the future. One of the solutions to these problems is the technology of signal transmission in visible light.

Сучасна тенденція бездротового зв'язку з постійно зростаючим попитом на більш високу пропускну здатність та повсюдне покриття, створюють високий попит на використання спектру радіочастотної зв'язку. Цей напрямок вимагає альтернативних засобів для пошуку додаткових можливостей зв'язку в майбутньому. Одним з варіантів вирішення цих проблем є технологія передачі сигналів по видимому світлу.

Інтерес бездротового зв'язку у видимому світлі (VLC-visible light communication) зріс одночасно з розробкою і використанням світлодіодних технологій. Багато авторів почали мати справу з різними аспектами які характеризують зв'язок у видимому світлі, особливо в відношенні модуляції і затемнення. Це призвело до першої стандартизації фізичного рівня і рівня MAC, ратифікованого IEEE (802.15.7) і включеної до Бездротові персональні мережі [1].

Видима частина спектру охоплює від 380 Нм до 780 Нм довжини хвилі, а частота $4,3 \times 10^{14}$ Гц. і $7,5 \times 10^{14}$ Гц. У технології VLC використовуються світлодіоди, оскільки їх інтенсивність струмів легко модулюється відносно їх аналогів. [2].

Даний тезис надає інструкції для реалізації випробувального стенду VLC за допомогою програмно конфігурованого радіо (SDR) який кепується за допомогою програмного забезпечення GNURadio.

Принцип роботи SDR пристроїв базується на цифровій обробці прийнятого радіосигналу і наступній його обробці у цифровому сигнальному процесорі або ПЛІС, керування роботою яких забезпечується від персонального комп'ютеру, до якого підключається пристрій. При цьому технологія прямого цифрового перетворення і прямого цифрового синтезу з діапазонними фільтрами дозволяє отримати максимально високі характеристики передавальна-приймального тракту [3,4].

GNURadio є вільним і відкритим джерелом програмного забезпечення, що розширює інструментарій та забезпечує можливості програмного радіомовлення. Він використовується в основному в якості програми

управління SDR пристрою, яка готує дані для обробки сигналу. Операція обробки сигналу закінчується пізніше спеціалізованим модулем. GNURadio пропонує легко перелаштовуємо радіосистему, що дозволяє користувачам створювати різні пристрої без необхідності покупки декількох дорогих радіостанцій. Його можна використовувати для створення додатків, отримання даних з цифрових потоків або передавати дані в цифрові потоки. Потім ці потоки передаються з використанням апаратних засобів.

GNURadio має фільтри, каналні кодери, елементи синхронізації, еквалайзери, демодулятори, вокодер, декодери і багато інших елементів (блоків). Також GnuRadio включає в себе спосіб підключення цих блоків і управління передачею даних від одного блоку до іншого.

Для дослідження передачі сигналів в оптичному тракті необхідно підключити персональний комп'ютер TX через USB під'єднати SDR трансивер, вихід якого через коаксіальний кабель під'єднаний до інжектору постійного струму (Bias-T) на який подається напруга 0,2V та до виходу якого під'єднана LED лампа з драйверами.

Для приймання оптичних сигналів необхідно підключити фотодетектор через коаксіальний кабель до SDR трансивер, який через USB роз'єм підключається до комп'ютера RX.

Блок схема передавача та приймача VLC представлені на рис.1.

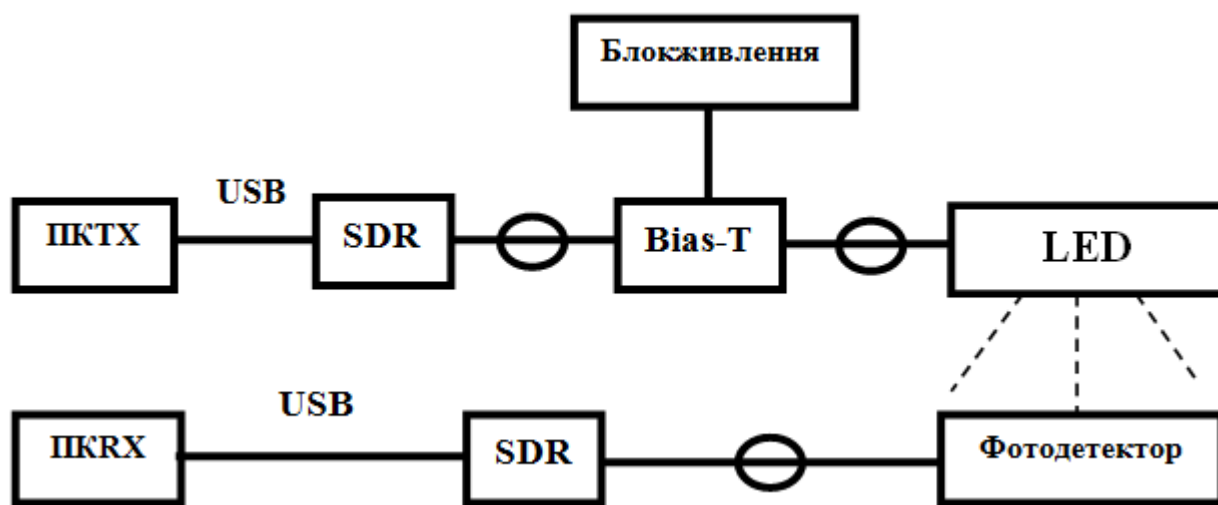


Рисунок 1. Блок схема дослідження передачі сигналів в оптичному тракті.

Для програмування SDR трансивера використовуємо програмне забезпечення GNURadio в якому за допомогою блоків збираємо схему передавача (рис. 2) та приймача (рис. 3).

Схема передавача складається з наступних блоків: блоку вхідних даних в якому вказується шлях до файлу який будемо передавати (File Source), пакетний кодер (Packet Encoder), Частотна модуляція Гауса з мінімальним зрушенням (GMSK Mod), блок керування трансивером, в даному випадку використовується трансивер USRP (USRP2 Sink), а також допоміжні блоки у яких встановлюється частота дискретизації (samp_rate), тип графічної оболонки (Options).

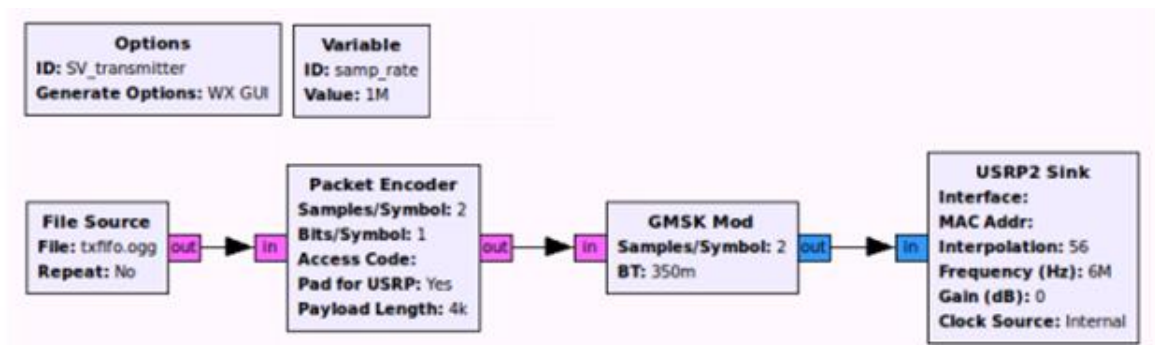


Рисунок 2. Блок схема передавача.

Схема приймача складається з наступних блоків: блок вхідних даних які приймаються на трансивер (USRP2 source), фільтр низьких частот (LowPassFilter), Частотна демодуляція Гауса з мінімальним зрушенням (GMSK Demod), пакетний декодер (PacketDecoder), блок запису вихідних даних в якому вказується шлях куди буде записаний файл.

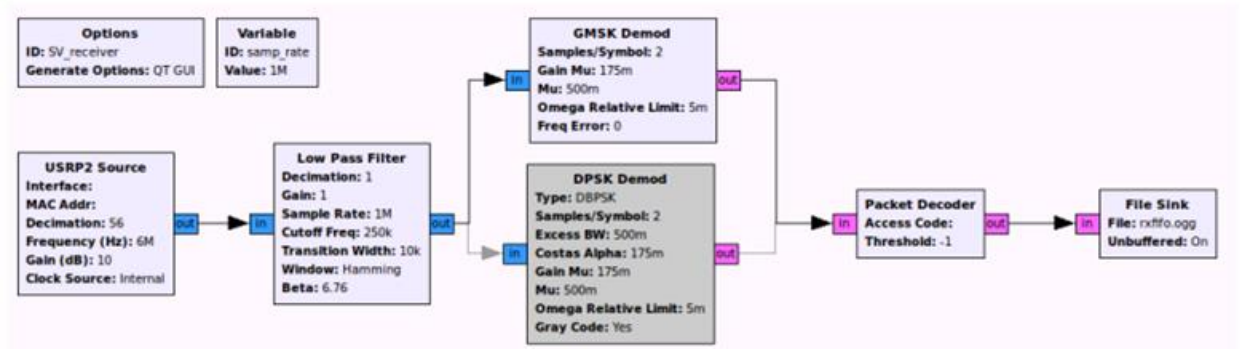


Рисунок 3. Блок схема приймача.

Системи SDR дають чудову можливість для подальших можливостей досліджень аналізу та навчання систем зв'язку, зокрема VLC. Також змінюючи блок схему в програмному забезпеченні GNURadio можливо проводити дослідження та порівняння різних типів модуляції та завадостійкого кодування.

Література

1. S. Rajagopal, R.D. Roberts, and L. Sang-Kyu, "IEEE 802.15.7 VisibleLightCommunication: ModulationSchemesandDimmingSupport," IEEE Commun. Mag., vol. 50, no. 3, pp. 72–82, 2012.
2. R.J. Drost and B. M. Sadler IEEE TransactionsonCommunications, vol. 62, pp. 1995–2005, 2014.
3. Літвінов Є.А., Авдєєнко Г.Л. «Використання SDR трансивера bladerfx40 для формування сигналів цифрового телебачення стандартів DVB-S та DVB-S2». Матеріали 13-ої МНТК конференції «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем» Київ, 2019р. С186-188.
4. O.I. Romanov, Y.S. Hordashnyk, T.T. Dong. Method for calculating the energy loss of a light signal in a telecommunication Li-Fi system. International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), 2017, p: 1 – 7.

АНАЛІЗ ВАРІАНТІВ ПЕРЕХОДУ ДО МЕРЕЖ НАСТУПНОГО ПОКОЛІННЯ З ВИКОРИСТАННЯ ТЕХНОЛОГІЇ NG-PON2

Данильченко В.О., Кононова І.В.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: vika.sp2222@gmail.com

Analysis of NG-PON2 next generation network transition options

An analysis of the current state of information telecommunication networks was built on the basis of new generation passive optical networks. Options for implementing NG-PON2 technology based on direct migration are proposed.

Сучасні технології надають достатньо високі швидкості, проте зі зростаючою кількістю нових підключених гаджетів, датчиків та іншого обладнання, цього може бути недостатньо. Виникає потреба в збільшенні швидкості та пропускної здатності інфотелекомунікаційної мережі, а також наданні та підтримки додаткових послуг.

Звертаючи увагу, що в мідних та оптичних мережах є певні обмеження, наприклад, GPON при такій тенденції не зможе забезпечити достатню ємність [1], тому для вирішення цієї проблеми необхідно виконати перехід до NG-PON2 (Next-Generation Passive Optical Network 2 – пасивна оптична мережа нового покоління) (рис. 1) – першої багатохвильової пасивної оптичної мережі [2].

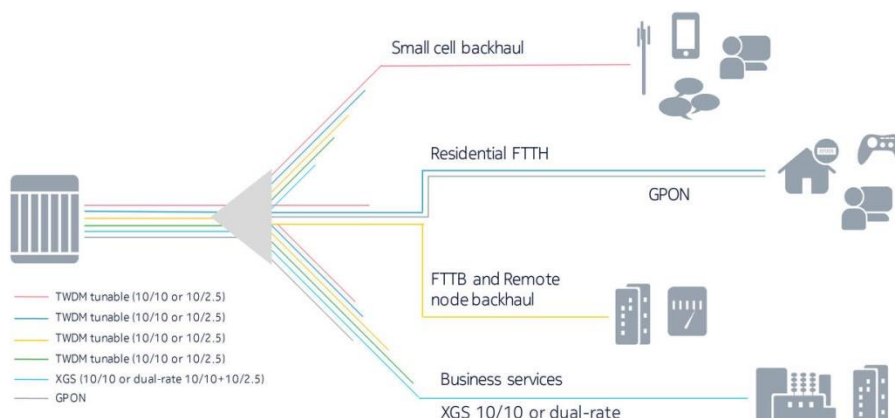


Рис. 1. Варіант переходу до NG-PON2.

Для досягнення поставленої мети необхідно зробити плавний перехід від існуючих систем PON (GPON) до NG-PON2. Співіснування двох поколінь PON може дозволити гнучку міграцію та розгортання за вимогами нових з'єднань PON без переривання обслуговування, а для забезпечення максимальної гнучкості системи NG-PON2 необхідно співіснування зі всіма технологіями PON на одній оптичній розподільній мережі (Optical Distribution Network – ODN).

Для полегшення співіснування різних поколінь технологій та забезпечення переходу до системи NG-PON2 вона повинна бути здатною повторно використовувати існуючі оптичні розгалужувачі потужності PON і повинні також працювати у використуваному спектрі, не зайнятому успадкованою PON. Проте, система NG-PON2 може повторно використовувати спектр, розміщений у існуючій PON системі, якщо не співіснують з цими PON-ми [3].

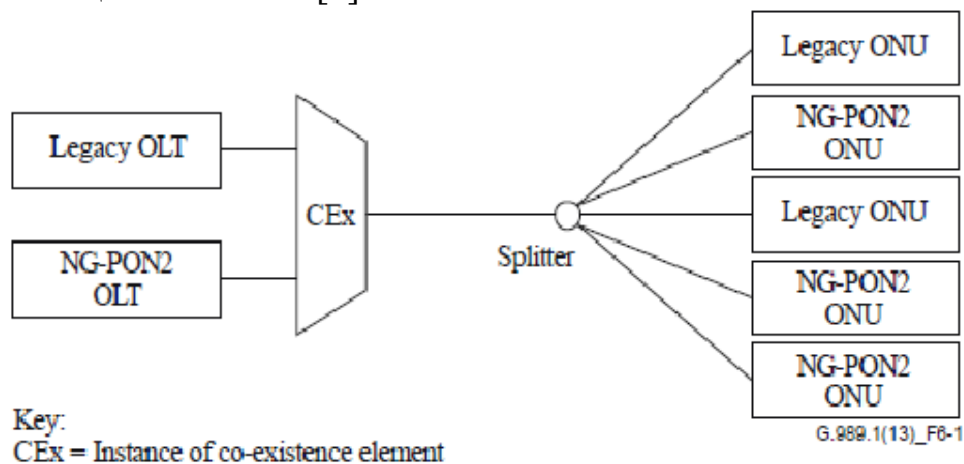


Рис. 2 Сценарій співіснування на ODN.

Проведений аналіз сучасної літератури показав, що на даний час існує 2 варіанти переходу до мереж наступного покоління. Перший варіант використання стандарту PON нового покоління (XG-PON), який може забезпечити показники пропускної здатності 10 Гбіт/с спадний потік і 2,5 Гбіт/с висхідний. Другий варіант, NG-PON2 в цьому стандарті впровадження спектрального мультиплексування забезпечить збільшення пропускної здатності до 40 Гбіт/с в низхідному і 40 Гбіт/с висхідному напрямках через кілька каналів 10 Гбіт/с/10 Гбіт/с в єдиній волоконно-оптичній інфраструктурі [1].

Перевагами технології NG-PON2 для використання її при переході до мереж наступного покоління є: сумісність з технологіями GPON і XGS-PON/XG-PON1; підтримка чотирьох довжини хвилі в первісному випуску, при цьому забезпечення можливості переходу на 8 довжин хвиль; підтримка налаштування оптики, яка забезпечує мобільність по всій довжині хвилі; підтримка різних видів трафіку; підтримка безлічі додатків і послуг, що підтримують PON; симетрія, низька затримка і надійність, життєво важливі для хмарних сервісів; підключення до бізнесу і мобільного зв'язку, а також покращена відмовостійкість і енергозбереження.

Проаналізувавши переваги та недоліки, в своїй роботі я пропоную використання технології NG-PON2 для таких областей використання: житлові, мобільні та бізнес послуги (рис. 3) використовуючи варіант міграції - пряма міграція.

Пряма міграція охоплює прямий шлях міграції відповідно до порядку генерації PON з GPON через XG-PON1 до NG-PON2. Передбачається

співіснування GPON та NG-PON2 на одній розподільній мережі (ODN), що є актуальнішим та більш економічно вигідним варіантом.

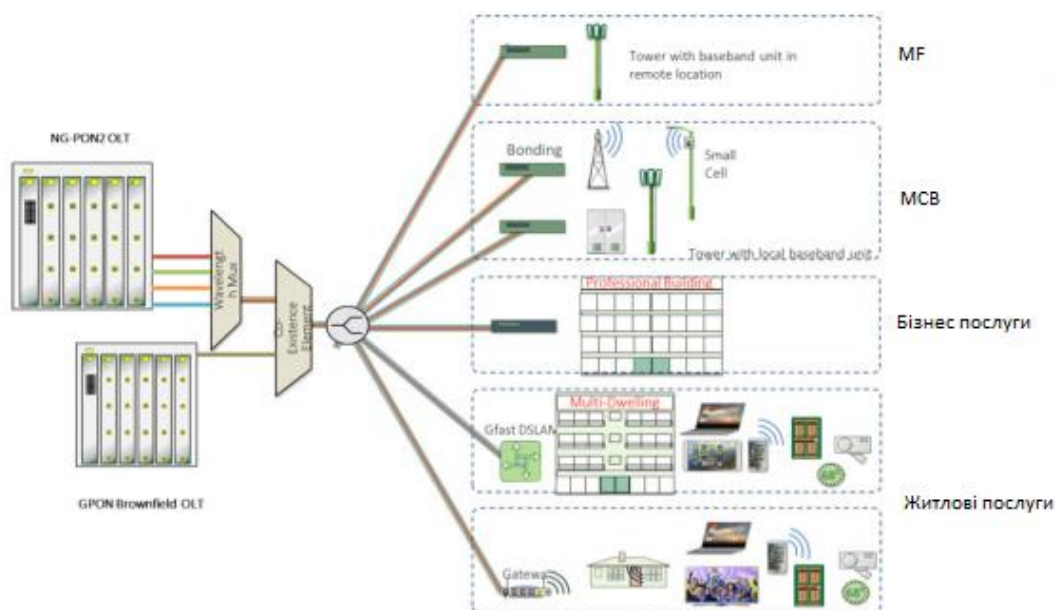


Рис. 3. Варіанти впровадження NG-PON2.

Необхідна міграція з GPON на XG-PON1 перед оновленням до NG-PON2. Цей варіант міграції можна реалізувати, видаливши GPON з ODN і повторно використати вікна довжини хвилі GPON, щоб включити технологію NG-PON2, що співіснує з XG-PON [3].

Отже, NG-PON2 пропонує постачальникам послуг значні переваги в порівнянні з іншими технологіями 10GPON. Так як NG-PON2 - це багатоканальна система PON, яка не тільки збільшує доступну ємність у волокні в 4 рази, але також завдяки підтримці налаштування модулів оптичних мереж (ONU) клієнтів забезпечує безпрецедентні переваги як операторам, так і користувачам. До яких відносяться підвищена продуктивність і доступність послуг, модель розгортання з оплатою в міру зростання, захисна комутація за довжиною хвилі, плавне оновлення програмного і апаратного забезпечення в центральному офісі, можливості енергозбереження. В результаті цієї гнучкості і поліпшеною продуктивності можливий повний перехід до оптичних мереж та можливості зниження її вартості.

Література

1. NG-PON2. The future of Passive Optical. Networking is Here (2018). Retrieved October 17, 2019.
2. Physical Layer Aspects of NG-PON2 Standards—Part 1: Optical Link Design [Invited] Wey, Jun Shan; Nasset, Derek; Valvo, Maurizio; Grobe, Klaus; Roberts, Hal; Luo, Yuanqiu; Smith, Joe, 2016.
3. 40-Gigabit-capable passive optical networks (NG-PON2): General requirements. Recommendation ITU-T G.989.1. 2013.

АНАЛІЗ ПРИНЦИПІВ ПОБУДОВИ MPLS L3 VPN

Литовченко К.А., Романов О.І.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського

E-mail: konstantinlitovchenko02@gmail.com; a_i_romanov@ukr.net

MPLS L3 VPN construction principles analysis

This article explores building a VPN network that runs on the third layer of the OSI model, based on the transmission protocol using MPLS tags. Description of the MPLS protocol. The overall infrastructure of a VPN system that benefits from such a system based on MPLS tags compared to using IPv4. More and more telecom representatives are moving to MPLS L3 VPN based jobs. The solution can be justified by a well-designed network architecture, high quality of service (QoS) and the degree of security of such a system.

У даній статті досліджується побудова VPN мережі, яка працює на третьому рівні моделі OSI, на базі протоколу передачі за допомогою міток MPLS. Опис роботи протоколу MPLS. Загальна інфраструктура системи VPN, вигоди такої системи побудованої на основі міток протоколу IPMPLS у порівнянні з використанням протоколу IPv4. Все більше представників телекомунікаційної сфери переходять на роботу, яка основана на MPLS L3 VPN. Рішення можна обґрунтувати добре продуманою архітектурою мережі, високою якістю послуг (QoS) та ступінню захищеності такої системи.

Рівень 3: постачальник послуг братиме участь в маршрутизації з клієнтом. Замовник запустить OSPF, EIGRP, BGP або будь-який інший протокол маршрутизації, ці маршрути можуть бути розділені з іншими сайтами клієнта. VPN: інформація про передачу даних від клієнтів повністю відокремлена та захищена від інших клієнтів, не авторизованих користувачів та направлена по мережі MPLS провайдера.

VPN на базі MPLS 3 рівня використовує однорангову модель, котра базується на протоколі граничного шлюза (BGP) для передачі інформації. Ця масштабована однорангова модель дозволяє корпоративним абонентам розповсюджувати дані про маршрутизації інших постачальників послуг, що приводить до значної економії ресурсів та зниженню складності операцій. Також система реалізована на протоколі MPLS, не потребує налаштувань всіх BGP на кожному маршрутизаторі, а лише на граничних роутерах, підключених до інших клієнтів або провайдерів, на відміну від IPv4. В VPN на базі IP використовується екземпляр віртуальної маршрутизації/пересилання наступного покоління (VRF), званий Easy Virtual Network (EVN). Це спрощує віртуалізацію мережі рівня 3 і дозволяє клієнтам забезпечити поділ трафіку й ізоляцію шляху в загальній мережі інфраструктури, усуваючи необхідність розгортання MPLS в мережі підприємства. EVN повністю інтегрований з традиційним MPLS-VPN або MPLS VPNomGRE.[1]

MPLS дозволяє створювати віртуальні приватні мережі Layer 3, не вдаючись дотунелюванню (GRE) та шифруванню (IPsec). MPLS VPN мережу ділить на дві області: IP мережі клієнтів і магістраль провайдера. Класична конструкція MPLS L3 VPN складається з наступних компонентів: граничні маршрутизатори провайдера PE, звернені до клієнтського обладнання CE, з'єднані між собою Р маршрутизаторами в MPLS домені. В принципі, Р маршрутизаторів може і не бути, необхідно щоб забезпечувалася зв'язність між PE.

MPLS L3 VPN інфраструктура (рис.1) передбачає забезпечення ізоляції розподілених клієнтських IP мереж в рамках VPN. Тобто забезпечується тільки обмін пакетами між IP мережами однієї VPN.

У термінах MPLS VPN окреме CE підключення називається сайтом. Кожен сайт являє собою окрему клієнтську підмережу, що входить в ту чи іншу VPN структуру. Кожна VPN логічно пов'язана з одним або більше комплексів маршрутизації та переадресації (VPN Routing and Forwarding instance - VRF).

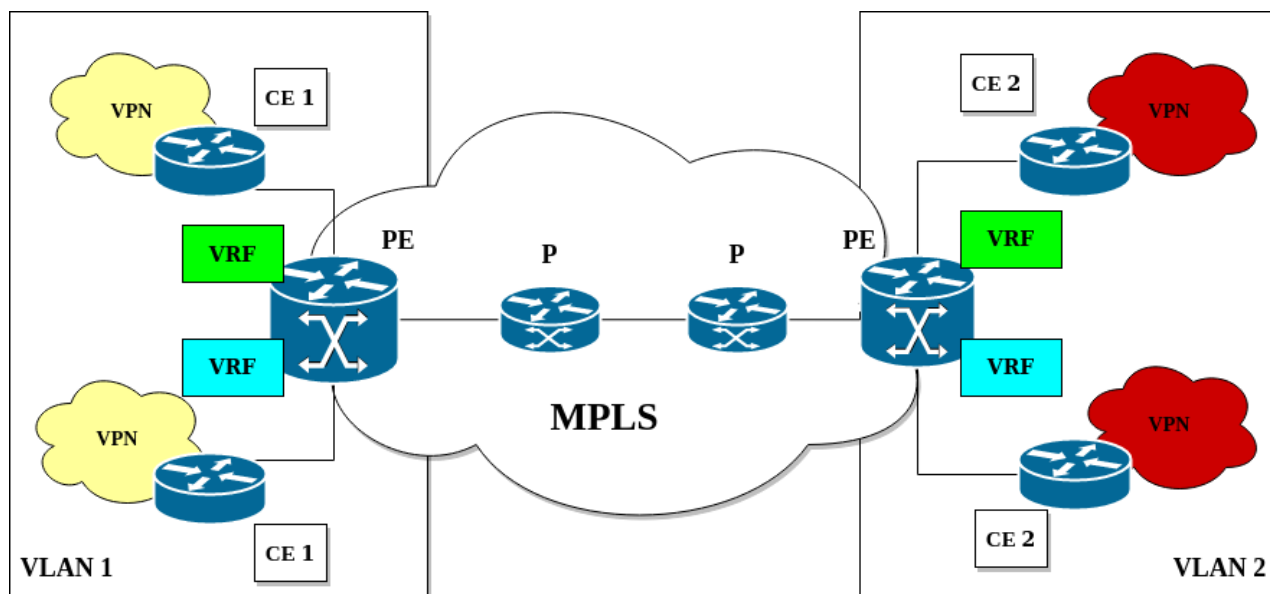


Рис. 1. Схема передачі VRF повідомлення між VLAN 1 та VLAN 2 за допомогою протокола MPLS.

Інтерфейси PE маршрутизаторів, звернені до CE, логічно пов'язані з індивідуальними VRF. Екземпляр VRF складається з таблиці маршрутизації (IPv4), отримана з неї CEF, набір інтерфейсів, які використовують VRF і побічна інформація. VRF таблиці IP маршрутизації використовуються для обміну інформацією про маршрути тільки всередині VPN мережі, тобто ззовні не можна здійснити пакетизацію на маршрутизатор, що знаходиться всередині VPN (цей маршрут просто невідомий).

В рамках MPLS L3 VPN в VPN включається IPv4 клієнтської підмережі. У межах однієї VPN не допускаються пересічні IPv4 адреси. Однак в різних VPN це допустимо. Звідси потенційна неоднозначність для PE маршрутизатора: різні VRF можуть містити однакові IPv4 адреси. Для отримання унікальних адрес (і відповідно маршрутів), так званих VPN-IPv4, використовується ідентифікатор VPN-Route Distinguisher (RD). VPN-IPv4 отримується за допомогою додавання до IPv4 ідентифікатора RD. В результаті PE оперує унікальними VPN-IPv4.

Для обміну маршрутною інформацією між VRF різних PE використовується MP-BGP протокол. MP-BGP маніпулює над VPN-IPv4 маршрутами. Таким чином, за допомогою MP-BGP отримуємо віртуальний зв'язок між PE (між VRF однакових VPN). Для задоволення політики експорту/імпорту додатково вводиться поняття адресата маршруту - Route Target (RT).

У підсумку виходить наступна схема. Кожен клієнтський сайт (інтерфейс на PE) має свою VRF (таблицю IPv4 маршрутизації). PE може дізнатися IP префікс клієнта різними способами (статична конфігурація, BGP, RIP, OSPF). PE поміщає IPv4 маршрут клієнта в VRF даного сайту. Крім того, за допомогою заздалегідь обраного ідентифікатора VPN, в які входить даний сайт, IPv4 маршрути (префікси)

перетворюються в VPN-IPv4 маршрути і поміщаються в MP-BGP. MP-BGP згідно з політикою імпорту/експорту пов'язує між собою всі PE маршрутизатори (їх VRF). У підсумку в VRF різних PE, але належать одній VPN, потрапляють всі маршрути з даної VPN. Причому в записах VRF Next-Hop є PE, який ніби пов'язаний між собою (віртуально за допомогою MPLS) [2].

Реальна передача пакетів (комутація) відбувається за допомогою MPLS. MPLS мітки використовуються наступним чином: пакет містить два рівня міток (використовується стек). Перша мітка направляє пакет до необхідного PE (next- hop), а друга вказує комплекс VRF, логічно пов'язаний з вихідним інтерфейсом CE маршрутизатора пункту призначення. Розглянемо на прикладі проходження пакетів в MPLS L3 VPN.

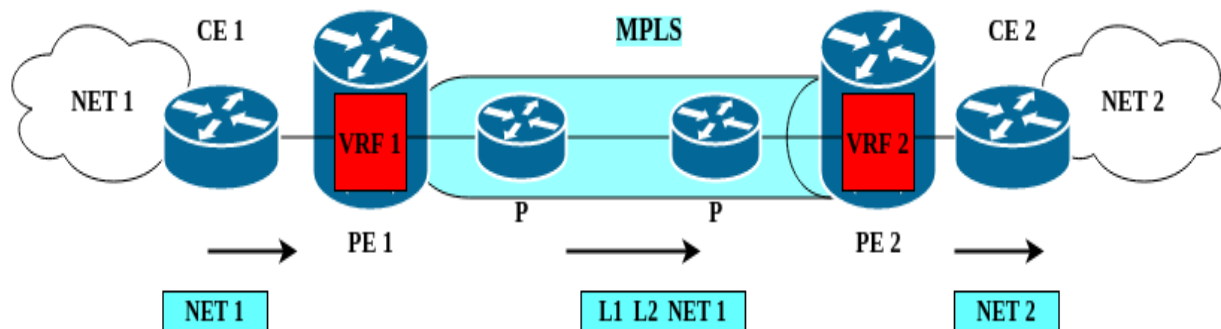


Рис. 2. Схема передачі MPLS пакетів по L3 VPN.

Припустимо, CE 1 посилає пакет для CE 2. Від CE 1 до PE 1 приходить пакет з DST = NET 2 (мережа за CE 2) та без міток. Даний пакет приходить із певного інтерфейсу і тому обробляється конкретною VRF 1. У VRF 1 є маршрут до NET 2 з NEXT-HOP — PE 2 і мітка VPN (мітка L1 для потрапляння в необхідну VRF 2 на PE 2). Мітку для досягнення PE 2 PE 1 шукає у своїй глобальній таблиці маршрутизації. Таким чином, PE 1 відправляє в сторону PE 2 пакет зі стеком міток: L2 для досягнення PE 2 як NEXT-HOP і L1 для досягнення потрібної VPN (VRF 2) на PE 2. За мітці L2 пакет доходить до PE 2 і вона там буде видалена. PE 2 по мітці L1 з'ясує який VRF використовувався для досягнення NET 2. У VRF 2 для NET 2 вказаний інтерфейс PE 2 - CE 2. В сторону CE 2 пакет передається без міток у вигляді IPv4.

Отже, було продемонстровано роботу протоколу MPLS в мережі VPN L3. Збільшується швидкість передачі даних за рахунок пропуску налаштувань всіх BGP на кожному маршрутизаторі, MPLS забезпечує повне розмежування адрес та передачі даних. Дана мережа є достатньо захищеною від зовнішніх загроз, проте її можна покращити вдаючись до тунелювання (GRE) та шифрування.

Література

1. Layer 3 VPNs [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/products/ios-nx-os-software/layer-3-vpns-l3vpn/index.html>.
2. Базовые сервисы технологии MPLS [Електронний ресурс] — Режим доступу до ресурсу: <https://nag.ru/articles/reviews/15448/bazovyie-servisyi-tehnologii-mpls.html>.

РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В МЕРЕЖІ ПІДПРИЄМСТВА НА ОСНОВІ МЕТОДІВ ЯКОСТІ ОБСЛУГОВУВАННЯ

Бондар О.Р., Верес Л.А.

Інститут телекомунікаційних систем

КПІ ім. Ігоря Сікорського, Україна

E-mail: sashashel@gmail.com

Developing security recommendations for the enterprise network based on quality of service methods

The article discusses the requirements for a modern enterprise network and characteristics of this network. Proved the importance of ensuring an adequate level of security in enterprise network. Described the concept of security and quality of service. Provided a method for protecting enterprise network using the Fail2ban software package.

У статті розглядаються вимоги до мережі сучасного підприємства, надається характеристика такої мережі. Обґрунтовується важливість забезпечення належного рівня безпеки в такій мережі. Надано опис поняття безпеки і якості обслуговування. Наведено метод захисту такої мережі з допомогою програмного пакету Fail2ban.

Сучасні мережі, незалежно від їх розміру, вимагають чіткого дотримання норм їх побудови. Вони повинні підтримувати велику кількість додатків і послуг, а також пристроїв з яких складається фізична інфраструктура. Основною функцією мережі є забезпечення доступу до ресурсів всіх пристроїв об'єднаних в мережу. Вимоги до мережі можуть бути різними в залежності від того де саме вона проектується і для кого. Великі підприємства потребують надзвичайно громіздких мереж з максимальним рівнем захисту і безліччю послуг які зменшують вартість обслуговування, полегшують адміністрування, або ж просто необхідні для успішного ведення бізнесу. В той же час для малих підприємств немає дуже суворих вимог до якості виконання мережі. Повільна робота такої мережі не буде мати таких катастрофічних наслідків у порівнянні з мережею великого бізнесу. Незважаючи на це, належне забезпечення безпеки є необхідним завданням в будь-якій мережі.

Ціль дослідження, запропонувати нетипові рішення для покращення рівня захисту мережі базованої на Linux-системі. Такі рішення зазвичай роблять злам мережі більш складним для потенційного злоумисника, так як є незвичайними і неочікуваними.

Безпека - найважливіша з вимог до мережі саме для підприємств,

особливо для великих. Мережа великої компанії обов'язково повинна бути захищена, так як, вона містить в собі важливу, часто навіть секретну, корпоративну інформацію. Зловмисники легко можуть вдертися в незахищену мережу, викрасти дані, привести мережу в неробочий стан і тим самим зірвати нормальну роботу підприємства, що призведе до значних збитків. Можна виділити два типи проблем з безпекою мережі: безпека мережевої інфраструктури і безпека інформації. Забезпечення безпеки інфраструктури означає захист всіх пристроїв, що забезпечують підключення до мережі, і попередження несанкціонованого доступу до програмного забезпечення керування, встановленого на них. Безпека інформації означає захист пакетів з даними, що передаються по мережі, а також захист інформації, що зберігається на пристроях користувачів. Для захисту інформації існує три основні вимоги: конфіденційність, цілісність і доступність. Інформація повинна бути доступна тільки авторизованим користувачам, інформація не повинна бути змінена або спотворена, до інформації повинен бути своєчасний і надійний доступ[1].

Якість обслуговування, поруч з безпекою, є основною темою даної роботи. По суті своїй, цей термін означає пріоритизацію трафіку. Тобто певні типи даних мають вищий пріоритет і передаються швидше. Для чого це необхідно. Якщо попит на канали зв'язку перевищує можливості мережі виникає перевантаження каналу. Коли таке трапляється, пакети не можуть одразу потрапити в канал передачі. Пристрої маршрутизації ставлять такі пакети в чергу в буфері пам'яті, до тих пір, доки канал не звільниться. Користувач в цей момент спостерігає велику затримку між запитом, наприклад до серверу, і відповіддю. На практиці це означає, що користувач змушений гаяти час не потрібне очікування. Для деяких випадків такі затримки допустимі, а от для інших зовсім навпаки. Це не критично, якщо доведеться декілька секунд почекати доки завантажиться поштовий клієнт. Проте такі затримки фатальні при передачі голосового або відео трафіку. Щоб такого не траплялося, якість обслуговування визначає певні типи трафіку які мають вищий пріоритет над іншими. Пакети з голосовим або відео трафіком завжди будуть першими в черзі на передачу, навіть якщо прийшли ну вузол останніми і опинились в кінці довгої черги[2].

Тепер слід більш детально розглянути поняття мережі підприємства. Мережа підприємства – це сукупність мереж і служб, призначених для надання захищеного мережного простору користувачам в межах підприємства[3]. Основними особливостями мережі підприємства є:

- 1) Ті ж самі засоби управління, що використовуються в мережах загального користування.

2) Доступ до інформації надається тільки обмеженій групі користувачів всередині локальної мережі підприємства. Ця локальна мережа відділена від глобальної мережі міжмережевими екранами.

3) Всередині мережі інформація поділяється на три типи. Офіційна (розповсюджується на рівні організації), групова(призначена для використання групою осіб), неофіційна(особиста інформація працівників).

4) Наявність централізованої системи керування мережею.

Узагальнена структура мережі підприємства представлена на рис.1.

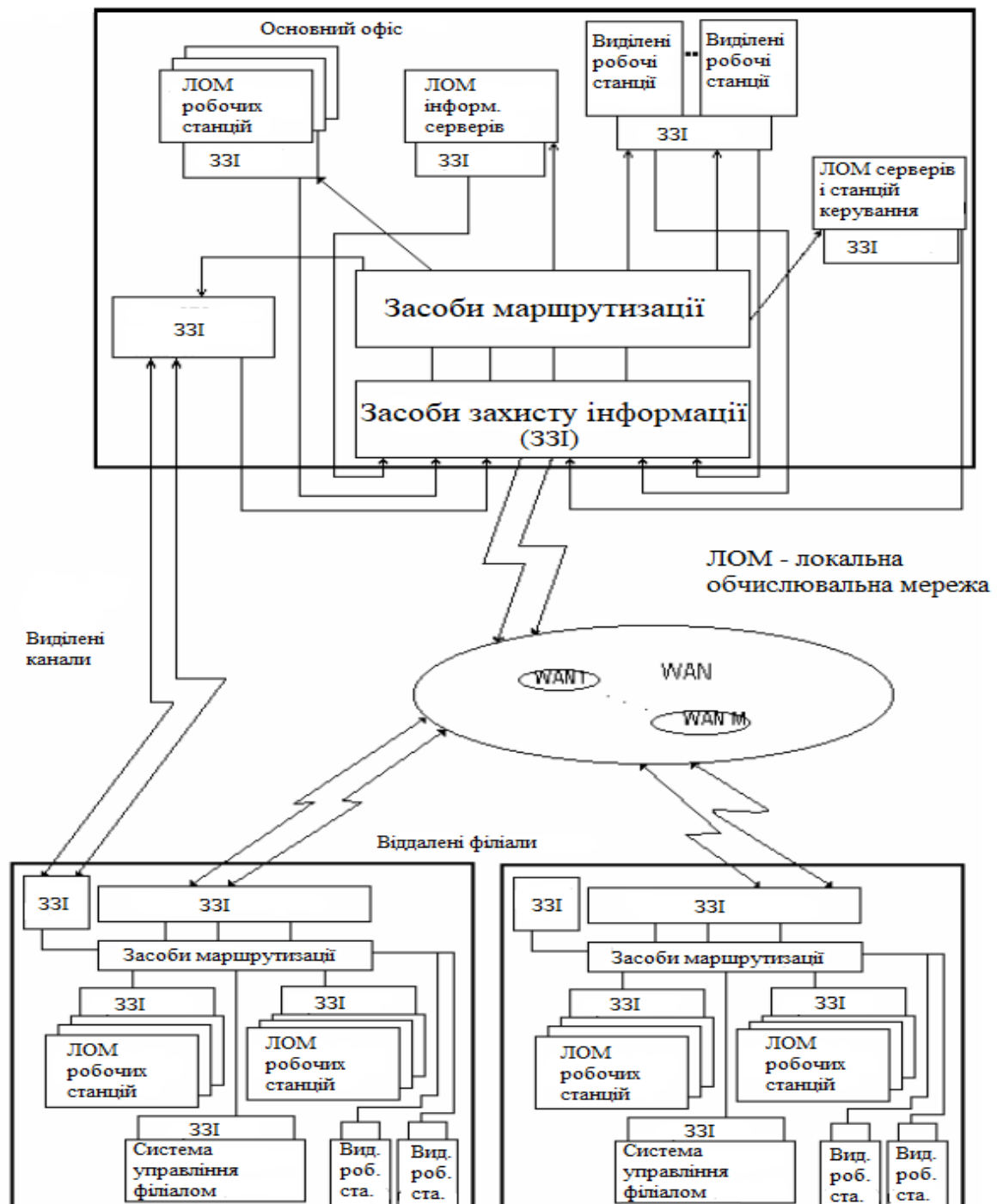


Рис.1. Узагальнена структура мережі підприємства.

Захист одного вузла мережі, як і всієї мережі, підключених до мережі Інтернет, від зовнішніх загроз, зазвичай не обмежується якимось одним апаратним або програмним засобом. Для забезпечення надійного захисту застосовуються комплекси які складаються з окремих програмних засобів. Такий спосіб є більш гнучким і дозволяє варіювати ступінь і рівень захищеності. В даній роботі буде застосовуватись захисний комплекс Fail2ban – програмний пакет, призначений для виявлення і запобігання спроб вторгнення в систему підключену до мережі. Fail2ban для своєї роботи використовує мережевий екран – firewall. В Linux-системі це iptables. Як варіант можна скористатися іншою підсистемою керування і відслідковування мережевих пакетів. Fail2ban виявляє і блокує окремі IP адреси з яких проводяться спроби несанкціонованого доступу до мережі. Ці адреси виявляються шляхом моніторингу файлів журналу – log-файлів. Це дозволяє захистити мережу або вузол мережі від «brute force» атак[4].

Описаний метод дозволяє підвищити рівень захищеності мережі підприємства. Він чудово доповнює існуючі методи захисту, ставлячи перед зловмисниками, додаткові складнощі при спробі злому мережі. Цей метод рекомендується застосовувати на приграничному маршрутизаторі мережі або безпосередньо на вузлі, що потребує захисту(наприклад сервер). Є сенс користуватись цим методом у всіх мережах, що мають доступ до мережі Інтернет.

Література

1. <https://www.csoononline.com/article/3285651/what-is-network-security-definition-methods-jobs-and-salaries.html>.
2. <https://searchunifiedcommunications.techtarget.com/definition/QoS-Quality-of-Service>.
3. Биячуев Т.А. Безопасность корпоративных сетей. Учебное пособие / под ред. Л.Г.Осовецкого - СПб.: СПбГУ ИТМО, 2004. - 161 с.
4. https://www.ibm.com/developerworks/ru/library/l-fail2ban_01/index.html.

МЕТОДИКА РОЗРАХУНКУ БЕЗВІДМОВНОЇ РОБОТИ СИСТЕМИ IMS НА БАЗІ ВІРТУАЛЬНИХ МАШИН

Романов О.І., Верес Л.А. Нестеренко М.М.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: veresleonid@gmail.com

Methods of calculating the unfinding operation of the IMS system on the basis of virtual machines

Previously, all telecommunications possessed one monolithic equipment complex, which, when operating at the operator's level, was practically impotent to expand horizontally (physically) so vertically (programmatically). And with the help of the server technology, it became available. I at the time of the new telecommunication ownership, the operators need more and less to scale, and there is little more than the least monolithic possession. In addition, when IMS is deployed, as far as the mobile operator is concerned, it is necessary to examine the vIMS (virtual IP Multimedia sub system).

Раніше все телекомунікаційне обладнання представляло собою один монолітний апаратний комплекс, який при збільшенні мережі оператора практично неможливо було розширити як горизонтально (фізично) так і вертикально (програмне). Але з розвитком серверних технологій це стало доступно. Тому при впровадженні системи IMS в мережі мобільного оператора сьогодні розглядаються в основному vIMS (virtual IP Multimedia sub system).

При розгортанні архітектури IMS на базі віртуальних машин дає оператору мережі мобільного зв'язку такі дві головні переваги - це масштабованість і надійність.

Під масштабуванням мається на увазі можливість легко і швидко змінити конфігурацію віртуального сервера: додати потрібну кількість процесорних потужностей, оперативної пам'яті або збільшити обсяг дискового простору. А вертикально - це розроблення або додавання нового програмного забезпечення.

Надійність телекомунікаційного обладнання - це властивість обладнання зберігати свою працездатність надавати послуги в певний інтервал часу. Використання vIMS дозволяє гнучка і швидко використовувати методи резервування обладнання з використанням ресурсів хмари.

Спираючись на ці дві переваги була розроблена метод підвищення надійності архітектури IMS і модель, яка дозволяє розрахувати показники її надійності.

Розглянемо архітектуру IMS яка працює в мережі 4G для надання послуги VoLTE (рис.1).

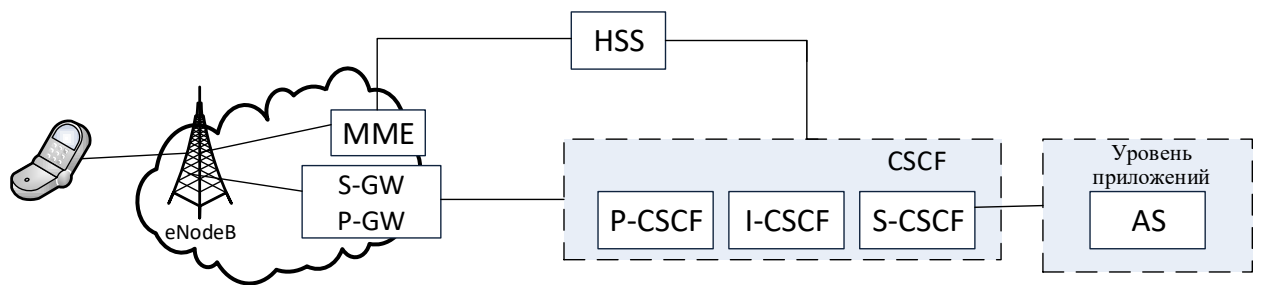


Рис. 1. Структура мережі 4G з інтеграцією в архітектуру IMS.

При використанні віртуальних машин ядро архітектури IMS набувають такого вигляду (рис.2):

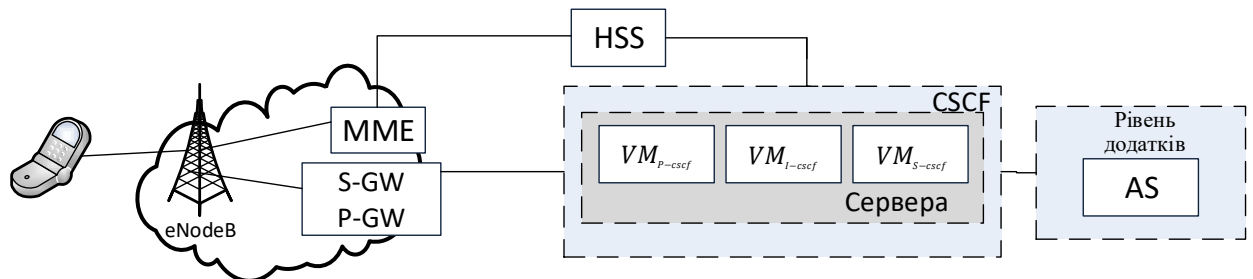


Рис. 2. Структура мережі 4G з заміною ядра IMS на віртуальні машини.

Тоді модель системи рис.2 може бути представленою у вигляді рис.3.

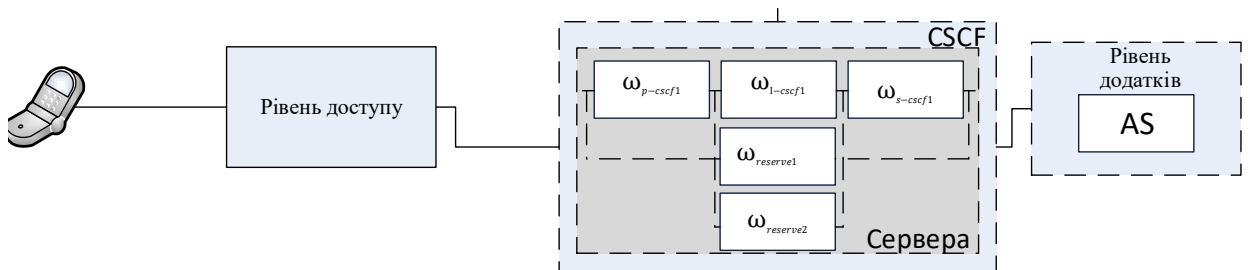


Рис 3 Модель ядра IMS на базі віртуальних машин.

Візьмемо до уваги що

$$\omega_{p-cscf1} = \omega_{I-cscf} = \omega_{S-cscf1} = \omega_{reserve1} = \omega_{reserve1} \text{ рівнозначні.}$$

На рис. 3 представлено модель ядра системи IMS "3 з 5". Система працездатна, якщо з п'яти функціональних елементів працюють будь-які три, чотири або всі п'ять. Ця система називається системи типу "m з n".

Розрахунок надійності системи "m з n" може проводитися комбінаторним методом, в основі якого лежить формула біноміального розподілу. Біноміальному розподілу підпорядковується дискретна випадкова величина k - число появ деякої події в серії з n дослідів, якщо в окремому досвіді ймовірність появи події становить p. При цьому ймовірність появи події рівно k раз визначається:

$$P_k = C_n^k p^k (1 - p)^{n-k}$$

де C_n^k - біноміальний коефіцієнт, званий "числом сполучень по k з n" (тобто скількома різними способами можна реалізувати ситуацію "k з n") який дорівнює:

$$C_n^k = \frac{n!}{k!(n-k)!}$$

Оскільки для відмови системи "m з n" досить, щоб кількість справних елементів було менше m, ймовірність відмови може бути знайдена по теоремі додавання ймовірностей для $k = 0, 1, \dots, (m-1)$:

$$Q = \sum_{k=0}^{m-1} P_k = \sum_{k=0}^{m-1} C_n^k p^k (1-p)^{n-k}$$

Аналогічним чином можна знайти ймовірність безвідмовної роботи як суму для $k = m, m+1, \dots, n$:

$$P = \sum_{k=m}^n P_k = \sum_{k=m}^n C_n^k p^k (1-p)^{n-k}$$

Розрахувати надійність архітектури IMS при роботі 3 елементів з 5, при умові $Q + P = 1$, можливе наступним чином:

$$\begin{aligned} P &= C_5^3 p^3 (1-p)^2 + C_5^4 p^4 (1-p)^1 + C_5^5 p^5 \\ &= 10p^3 (1-p)^2 + 10p^4 (1-p)^1 + p^5 \end{aligned}$$

Ймовірність відмови тієї ж системи дорівнює:

$$Q = 1 - P$$

Таким чином, використання моделі, параметрів надійності системи та наведених формул дозволяє розрахувати показники надійності системи vIMS при використанні різних конфігурацій системи управління. Наведено приклад розрахунку, коли в ядрі системи є п'ять елементів з яких працюють три.

Література

1. Mariia Skulysh, Romanov Oleksandr. The structure of a mobile provider network with network functions virtualization. // Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 2018 14th International Conference on. IEEE, 2018 - Pages: 1032 - 1034 DOI: 10.1109/TCSET.2018.8336370.
2. Abhayawardhana V.S., Babbage R. A traffic model for the IP Multimedia Subsystem (IMS) // 2007, IEEE Magazine, – C.783 – 787.
2. Скулиш М.А., Романов О.І., Глоба Л.С. Принцип обслуговування потоків у гетерогенному телекомунікаційному середовищі //Скулиш М.А., Романов О.І., Глоба Л.С. //Записки університету ім. В.І. Вернадського, - Том 29 (68) № 2 – 2018 –С. 92-98.
3. O.I. Romanov, M.M. Nesterenko, L.A. Veres. IMS: Model and calculation method of telecommunication network's capacity // Proceedings of the 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo) 11-15 Sept. 2017 Year, Odessa, Ukraine. - IEEE Conference Publications (IEEE Xplore Digital Library, DOI: 10.1109/UkrMiCo.2017.8095412), 2017. – P. 1-4.
4. Gonzalo Camarillo, Miguel-Angel García-Martín. The 3G IP Multimedia Subsystem (IMS): Merging the Internet and the Cellular Worlds by. (John Wiley& Sons, 2006, ISBN 0-470-01818-6).

АРХІТЕКТУРА МЕРЕЖІ IP-ТЕЛЕФОНІЇ НА ОСНОВІ SOFTSWITCH

Нестеренко М.М., Коломійчук О.А., Фесьоха Н.О.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут

E- mail: nikolaiy.nesterenko@gmail.com, sasik14gabo@gmail.com, nadya_viti@i.ua

Architecture of IP-telephony network with using softswitch

IP-telephony technology has become widespread through the convergence of telephone networks, cellular networks and IP networks. As, core used Softswitch, which in turn implements the principle of combining all types of signaling and integration of heterogeneous network.

На сьогоднішній день технологія IP-телефонії набула широкого розвитку за рахунок конвергенції телефонних мереж, мереж операторів стільникового зв'язку та мереж стеку *TCP/IP*. В основу концепції IP-телефонії покладено можливість передачі голосової та мультимедійної інформації в одній мережі.

Це означає, що маючи доступ до приватної/глобальної IP-мережі використовуючи канали передачі даних можна також передавати і голосовий трафік, це дозволяє реалізувати інтеграцію різномірних мереж та надання альтернативних інтелектуальних послуг телефонії рис. 1.

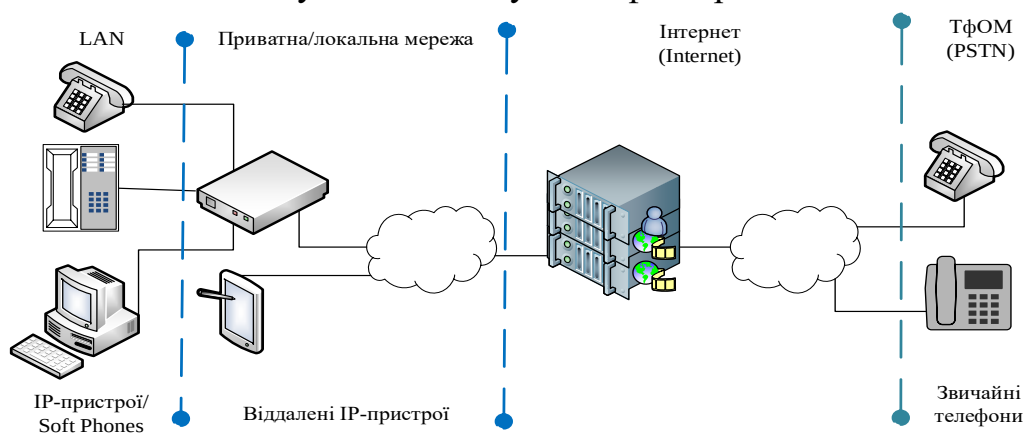


Рис. 1. Приклад використання IP-телефонії.

Одним із перших кроків до інтеграції різномірних мереж стало використання технології гнучкого програмного комутатора *Softswitch*. В основі успіху даного методу лежить можливість *Softswitch* транслювати (перетворювати) різні протоколи сигналізації як однотипних мереж, так і різнотипних мереж. Використання *Softswitch* дозволяє вирішити проблему взаємодії транспортних шлюзів (медіашлюзів) з різними системами сигналізації. В певній мірі *Softswitch* можна вважати не лише частиною

обладнання мережі, а мережевою архітектурою побудови мережі IP-телефонії.

До списку протоколів які використовуються в *Softswitch* для організації взаємодії в мережі IP-телефонії, можна віднести: *SIP*, *OKC7*, *H.323* (сигналізація управління з'єднанням); *E-DSS1*, *V5* (протокол абонентського доступу); *R1.5* (сигнальні канали), *MGCP* і *Megaco/H.248* (протокол сигналізації та управління транспортними шлюзами); *SIP-T* і *BICC* (протоколи сигналізації взаємодії між комутаторами *Softswitch*).

Згідно до еталонної архітектури *Softswitch*, розробленої консорціумом *IPCC* виділяються 4 площини функціонування: транспортна; управління обслуговуванням викликів і сигналізації; послуг і додатків; експлуатаційного управління рис. 2.

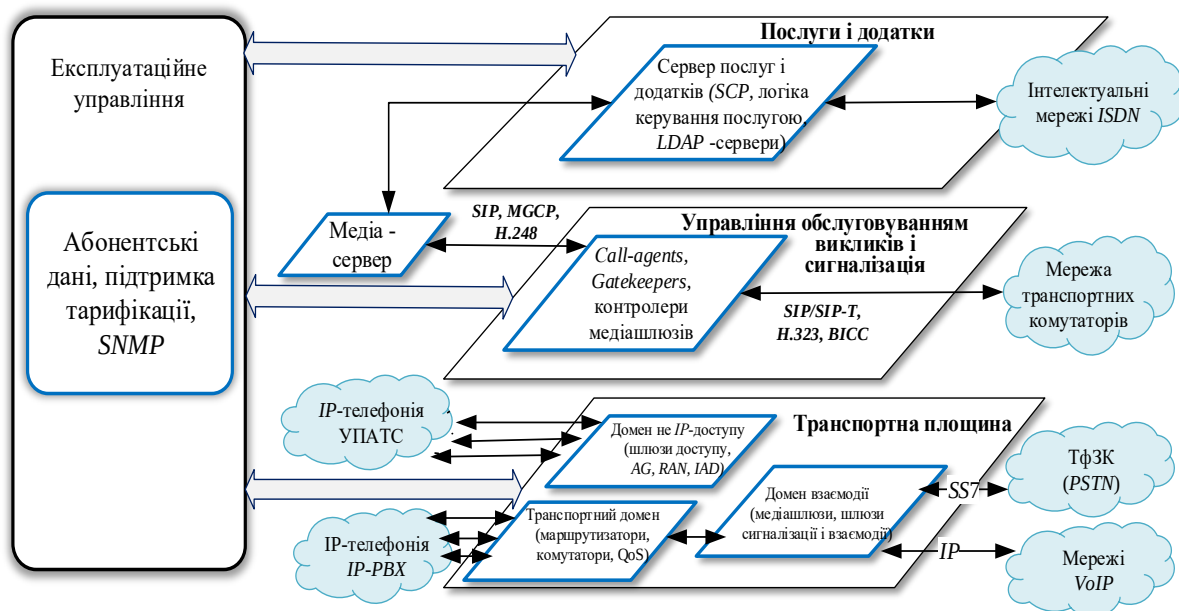


Рис. 2. Архітектура *Softswitch*.

Як видно із рис. 2 домен транспортування по протоколу IP підтримує магістральну мережу і маршрутизацію для переносу пакетів через мережу IP-телефонії. До нього відносять комутатори, маршрутизатори, а також засоби забезпечення якості обслуговування QoS. На площині експлуатаційного управління підтримуються функції взаємодії з іншими площинами по одному із стандартних протоколів (наприклад *SNMP*) або по внутрішніх протоколах та інтерфейсах *API*. До функцій, які також виконуються на цій площині відносяться: активізація абонентів та послуг, техобслуговування, білінг і т.д.

До функціональних об'єктів архітектури *Softswitch* відносяться логічні об'єкти мережі IP-телефонії (рис. 3).

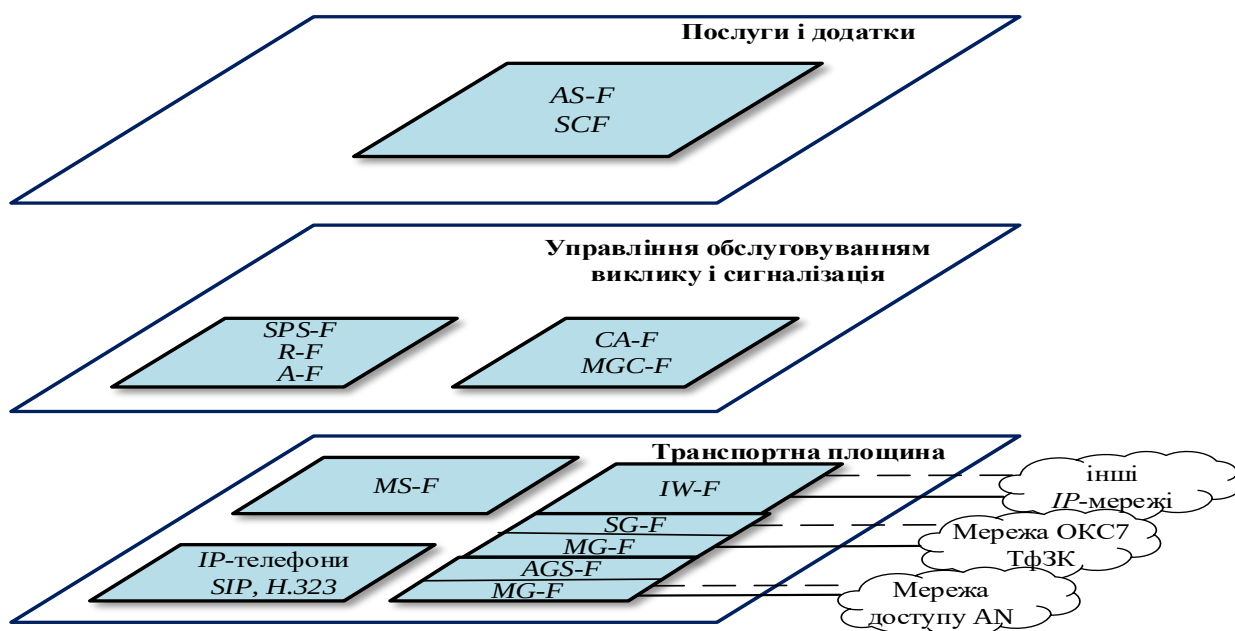


Рис. 3. Основні функціональні об'єкти *Softswitch*.

Всього виділяють 12 основних функціональних об'єктів (ФО): *Application Server Function* (AS-F) – ФО сервера додатків; *Service Control Function* (SC-F) – ФО управління послугами; *SIP Proxy Server Function* (SPS-F) – ФО проксі-сервера SIP; *Routing Function* (R-F) – ФО маршрутизації виклику; *Accounting Function* (A-F) – ФО обліку, авторизації та аутентифікації; *Call Agent Function* (CA-F) – ФО управління шлюзом; *Media Gateway Controller Function* (MGC-F) – ФО контролера медіашлюзів; *Media Server Function* (MS-F) – ФО транспортного сервера; *InterWorking Function* (IW-F) – ФО взаємодії; *SG-F* (*Signaling Gateway Function*) – ФО сигналізації; *MG-F* (*Media Gateway Function*) – ФО медіашлюзу; *Access Gateway Signaling Function* (AGS-F) – ФО сигналізації шлюза доступу.

Вище приведені підходи обумовили доцільність використання *Softswitch* в *Next Generation Networks* (NGN) та класичних IP-мережах. Оскільки *Softswitch* можна визначати, як програмний комутатор, який виконує задачу щодо передачі даних між різними типами мережа, а саме від звичайної телефонії (PSTN) до мережі Internet. В більшості випадків *Softswitch* встановлюється, як програмне забезпечення, на серверне обладнання необхідної потужності для якісного обслуговування абонентів. Відповідно до

цього *Softswitch* являється інтеграційним та інтелектуальним ядром мереж *IP*-телефонії.

До списку переваг даної технології в сучасних умовах можна віднести: універсальність (сюди можна віднести ряд таких функцій, як встановлення з'єднання, моніторинг елементів мережі, тарифікація та контроль з'єднання); низька вартість (як і для реалізації в системі, так і при наданні послуг тобто дозволяє використання існуючого мережевого обладнання); розширюваність (можливість легкого додавання послуг і т.д.); масштабованість (дозволяє змінювати кількість користувачів та максимальне значення трафіку за рахунок переконфігурування обладнання); гнучкість (робить доцільним використання даної технології як в приватних так і глобальних мережах); тарифікація (забезпечує можливість встановлення різних послуг і умов нарахування плати за їх використання окремо для кожного користувача).

Як висновок, при побудові мережі *IP*-телефонії *Softswitch* може бути використаний як інтеграційна платформа для сполучення існуючих різноманітних мереж, що в свою чергу дозволить розширити спектр послуг користувачам мережі за рахунок використання переваг *IP*-технологій. Також необхідно відмітити перспективність *IP*-телефонії за рахунок здешевлення надання послуг кінцевим користувачам. Однак, широке використання програмно-апаратних *Softswitch* має ряд труднощів у зв'язку із препроорітарними рішеннями різних вендорів мережевого обладнання і не сумісності їх між собою.

Література

1. Романов О.І., Нестеренко М.М., Гордашник Є.С. Аналіз функціональних особливостей побудови *IP*-мереж на базі *Softswitch* // Збірник наукових праць ВІТІ. – Київ, 2015. – Вип. №1 – С. 69 – 80.
2. Гольдштейн Б.С., Кучерявый А.Е. Сети связи пост-NGN СПб.: БХВ-Петербург, 2013. – 160 с.
3. А.А. Аттик, А.Б. Гольдштейн, Б.С. Гольдштейн Протокол Megaco/H.248: Справочник. – СПб.: БХВ Петербург, 2014. – 816 с.
4. Романов О.І., Нестеренко М.М., Верес Л.А., Гордашник Є.С. Модель розрахунку пропускної спроможності *IP*-мультимедійної підсистеми (IMS) // Збірник наукових праць ВІТІ. – Київ, 2017. – Вип. №2 – С. 92 – 100.
5. ADeart V.Y. Multiservice network. 2011. (*Softswitch / IMS*). Moscow: Briz-M, 2011. 198 p.

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ ASON В СУЧАСНИХ ТРАНСПОРТНИХ МЕРЕЖАХ

Тріска Н.Р.

Інститут телекомунікаційних систем КІП ім. Ігоря Сікорського
E-mail: ntriska@ukr.net

The deployment of ASON technology in the modern transport network

The perspectives of ASON (Automatically Switched Optical Network) technology deployment in the modern SDN-based transport networks are considered. The illustrative example of automatic network reconfiguration using ASON principles is presented.

Однією з основних світових тенденцій розвитку телекомунікаційних мереж є адаптація існуючої мережевої інфраструктури для переходу на перспективні технології 5G [1]. З точки зору транспортної мережі це передбачає впровадження програмно-конфігурованої архітектури SDN^[1] з віртуалізацією мережевих функцій NVF^[2]. Основні принципи побудови транспортних мереж на засадах SDN визначено в Рекомендації ITU-T G.7702 [2].

Концепція SDN/NVF може бути реалізована в існуючих транспортних мережах за допомогою різних апаратних і програмних засобів, але будь-яке технічне рішення має забезпечувати широкі можливості управління роботою складної багаторівневої мережі незалежно від використовуваних технологій та типу обладнання. Основний акцент робиться на таких функціях, як віртуалізація роботи мережі (відокремлення послуг, що надаються споживачам, від засобів передавання інформації), оптимізація використання ресурсів мережі та забезпечення надійності (зокрема, відновлення в аварійних ситуаціях зі збереженням необхідного рівня якості надання послуг).

Прикладом вдалого технічного рішення для реалізації концепції SDN в транспортній мережі є технологія ASON^[3] (оптична мережа з автоматичною комутацією). Вона достатньо добре відпрацьована і стандартизована в ITU-T (зокрема, в Рекомендації G.8080/Y.1304 [3]), а в контексті впровадження SDN застосування технології ASON набуває особливої актуальності. ASON забезпечує автоматизацію управління ресурсами мережі і підключеннями до неї на основі динамічних правил, що спираються на сигналізацію між користувачем і елементами мережі.

Логічна архітектура ASON може бути розділена за трьома площинами – рівнями: транспортний, оперативного управління та технічного обслуговування. *Транспортний рівень* представлений комутаторами (оптичними або іншими), які забезпечують транспортування даних користувача через організовані підключення.

^[1] SDN – Software Defined Networking

^[2] NVF – Network Function Virtualization

^[3] ASON – Automatically Switched Optical Network

Рівень оперативного управління відповідає за виділені в кожен конкретний момент часу ресурси і управління підключеннями в мережі ASON. На цьому рівні виконуються такі функції:

- забезпечення швидкого та раціонального конфігурування з'єднань транспортного рівня мережі – як комутованих, так і програмованих постійних (тривалих) з'єднань;
- перебудова або модифікація з'єднань, що були створені раніше за попередніми зверненнями / запитами;
- виконання дій з відновлення з'єднань.

Для створення з'єднання в мережі ASON необхідна взаємодія кількох складових – вузлів, яка може відбуватись за різними алгоритмами (ієрархічна або покрокова маршрутизація). Для різних форм управління трактами характерні різні принципи розподілу ресурсів між вузлами та взаємозв'язку між контролерами з'єднань CC (Connection Controllers). Якщо у маршрутизатора – контролера маршрутизації RC (Routing Controller), до якого надійшов запит на з'єднання, недостатньо інформації для формування відповідного маршруту, він може зв'язатися з іншими маршрутизаторами RC, використовуючи відповідний запит.

Налаштування з'єднання в мережі ASON здійснюється за допомогою спеціальної програми (логічного елемента), що управляє ресурсами трактів – LRM^[1] (менеджер лінійних ресурсів). В основу роботи LRM покладено матрицю зв'язків, яка містить інформацію про всі з'єднання елементів мережі та автоматично поновлюється в режимі реального часу. Це дозволяє транспортній мережі оперативно реагувати на аварійні ситуації, спрямовуючи трафік за оптимальними резервними маршрутами.

Рівень технічного обслуговування відповідає за управління ресурсами рівня оперативного управління (зокрема, управління конфігурацією ресурсів, зонами маршрутизації, транспортними ресурсами і правилами переключення), а також за управління функціонуванням, безпекою та відстеженням рахунків.

На рис. 1 наведено приклад автоматичної реконфігурації мережі ASON з 8 вузлів в разі вилучення з матриці з'єднань LRM однієї з'єднувальної лінії (ЗЛ) (наприклад, внаслідок пошкодження оптичного волокна на відповідній ділянці). На рисунку представлено матриці зв'язків / віддалень та схеми зв'язку, побудовані в програмному середовищі Matlab для нормального режиму роботи мережі та для аварійної ситуації (вилучення ЗЛ між вузлами В та Н). Для обох випадків розраховано середню мережеву зв'язність $\rho = M / N$ (де N – кількість вузлів в мережі, M – кількість наявних зв'язків між вузлами). Можна бачити, що після реконфігурації збереглися з'єднання між всіма вузлами (тобто забезпечується надійність роботи мережі за критерієм $N - 1$, хоча довжина деяких маршрутів збільшилась, а показник мережевої зв'язності дещо зменшився.

^[1] LRM – Link Resource Manager

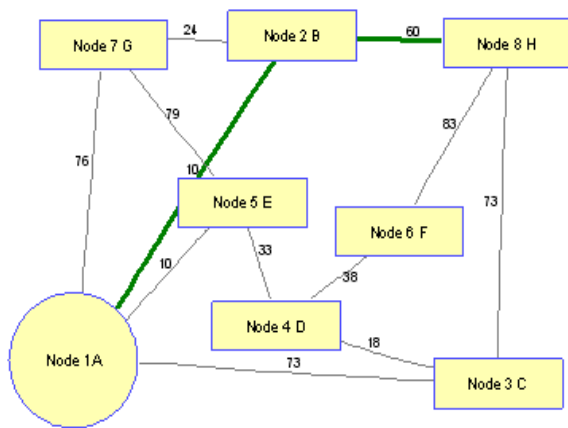
Матриці зв'язності/ віддалень та схеми зв'язку

Вихідна матриця

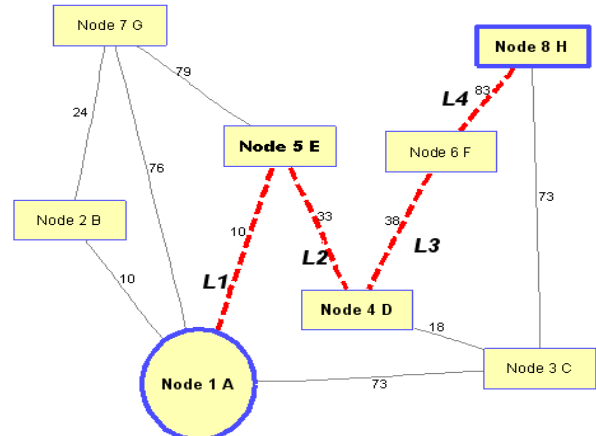
	A	B	C	D	E	F	G	H
A	0	10	73	0	10	0	76	0
B	0	0	0	0	0	0	24	60
C	0	0	0	18	0	0	0	73
D	0	0	0	0	33	38	0	0
E	0	0	0	0	0	0	79	0
F	0	0	0	0	0	0	0	83
G	0	0	0	0	0	0	0	0
H	0	0	0	0	0	0	0	0

Аварійна матриця (вилучена ЗЛ В-Н)

	A	B	C	D	E	F	G	H
A	0	10	73	0	10	0	76	0
B	0	0	0	0	0	0	24	0
C	0	0	0	18	0	0	0	73
D	0	0	0	0	33	38	0	0
E	0	0	0	0	0	0	79	0
F	0	0	0	0	0	0	0	83
G	0	0	0	0	0	0	0	0
H	0	0	0	0	0	0	0	0



Зв'язок **A-B-H** $L=70$ км
 $\rho=1,5$



Зв'язок: **A-E-D-F-H** $L=134$ км
 $\rho=1,4$

Рис. 1. Приклад автоматичної реконфігурації мережі ASON.

Слід зазначити, що основні засади технології ASON добре узгоджуються з перспективною концепцією побудови транспортних мереж SDN. Впровадження технології ASON завдяки її гнучкості, динамічності та широким можливостям в частині резервування, дозволяє забезпечити оптимальне використання ресурсів мережі та високі показники надійності, що відповідають рівню мережі операторського класу.

Література

1. Тріска Н.Р. Актуальні завдання підготовки телекомунікаційних мереж до впровадження стандарту 5G. – Тринадцята Міжнародна науково-технічна конференція “Перспективи телекомунікацій” (ПТ-2019), 15-19 квітня 2019 р. Матеріали конференції. – ІТС НТУУ “КПІ”. – С. 131-133.
2. ITU-T Recommendation G.7702 (03/2018) Architecture for SDN control of transport networks.
3. ITU-T Recommendation G.8080/Y.1304 (02/2012) Architecture for the automatically switched optical network.

ВИКОРИСТАННЯ ПРОГРАМНОГО ПАКЕТУ SYNC ARCHITECT ДЛЯ ПРОЕКТУВАННЯ МЕРЕЖ СИНХРОНІЗАЦІЇ

Тріска Н.Р.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського

E-mail: ntriska@ukr.net

The application of SYNC ARCHITECT program for synchronization networks design

The benefits of synchronization network design tool Sync Architect are considered. This tool allows optimizing the synchronization network resources as well as network planning and operation processes. The experience of use of Sync Architect in the academic activities in Institute of Telecommunication Systems is presented.

Сучасні телекомунікаційні мережі зазвичай мають досить складну структуру і використовують різноманітне обладнання систем передавання та комутації багатьох виробників. На сучасному етапі, коли відбувається адаптація мережевої інфраструктури до роботи за стандартами 5G з впровадженням нових послуг та платформ управління, операторам важливо забезпечити спадкоємність та співіснування технологій і разом з тим оптимально застосувати нові підходи до планування та експлуатації мереж [1]. З ускладненням структури сучасних мереж та впровадженням програмно-конфігурованої архітектури мереж на засадах концепції SDN, особливої актуальності набувають задачі забезпечення надійності та відновлюваності мережі, моніторингу та оперативного реагування на аварійні ситуації. Це, зокрема, стосується і аспектів синхронізації та розповсюдження точного часу в умовах пакетної мережі з асинхронним способом передавання.

Планування складної мережі “вручну” може виявитись неоптимальним та/або призвести до помилок, що впливатимуть на якісні показники. Тому на практиці на етапах планування, впровадження та технічної експлуатації телекомунікаційних мереж широко застосовуються спеціалізовані програмні пакети, які дозволяють оптимізувати процес планування, а також моделювати роботу мережі та/або здійснювати її моніторинг в режимі реального часу. Вдалим прикладом такого підходу в сфері планування та експлуатації мереж синхронізації є програмний пакет Sync Architect (розробка британської компанії Horsebridge), який протягом тривалого часу використовується багатьма операторами телекомунікацій. Програмний пакет Sync Architect дозволяє:

- здійснювати планування мережі синхронізації або її фрагменту на базі зручного інтерфейсу користувача, що представляє топологію мережі синхронізації в наочній і зручній для аналізу формі (див. рис. 1);

- створювати і використовувати базу типових елементів системи синхронізації різного рівня – від первинних пристроїв синхронізації класу PRC (рис. 2) до генераторного обладнання нижчого рівня, вбудованого в мультиплексори SDH або комутатори Ethernet (рис. 3). Модель дозволяє

деталізувати всі основні характеристики пристрою синхронізації (кількість входів та виходів, кількість та тип внутрішніх генераторів, налаштування схем перемикання сигналів тощо), що дозволяє врахувати особливості конкретних моделей обладнання;

- налаштовувати обмін повідомленнями про статус сигналу синхронізації – SSM з метою запобігання петель (циклів) синхронізації.

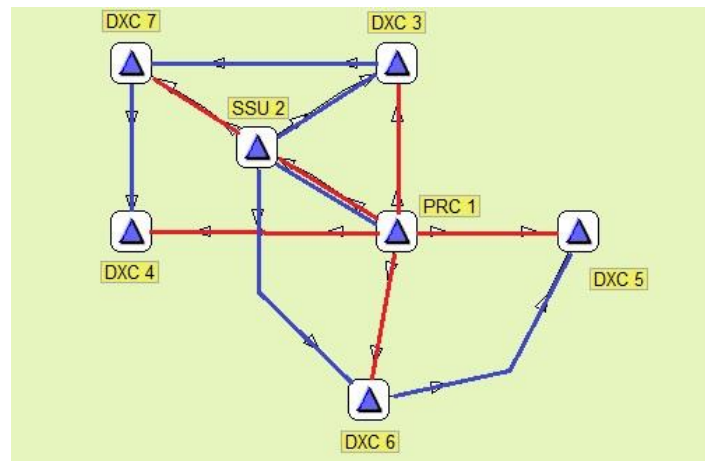


Рис.1. Приклад схеми фрагменту мережі синхронізації, побудованої в Sync Architect.

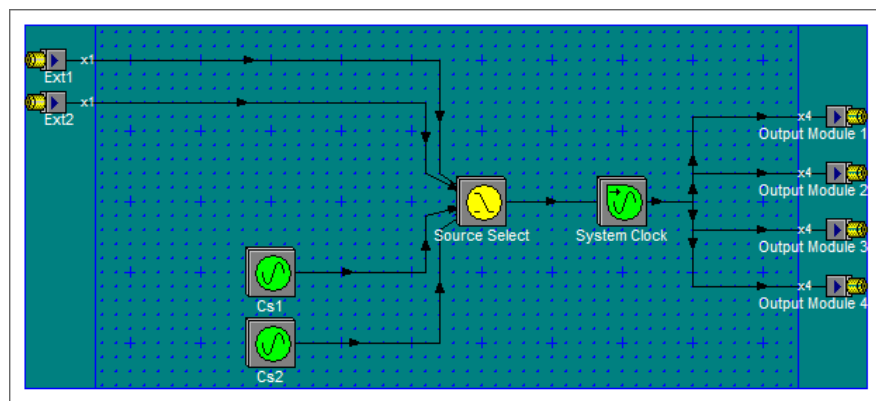


Рис.2. Приклад моделі пристрою PRC^[1] з бази елементів Sync Architect.

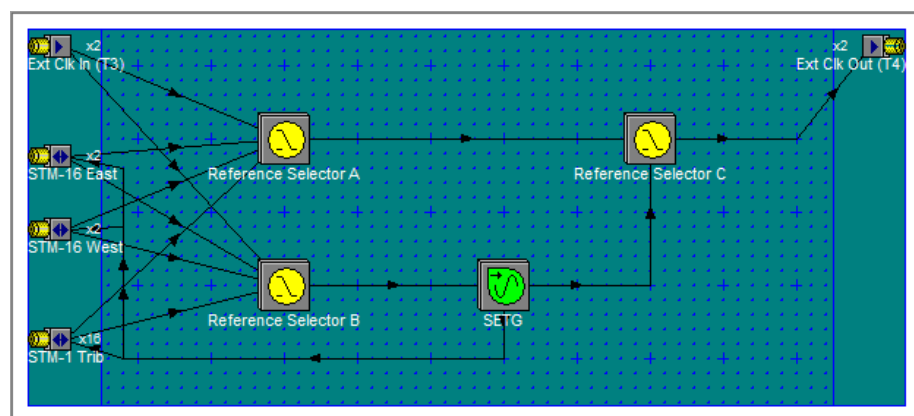


Рис.3 Приклад моделі генераторного обладнання мультиплекера SDH (SEC^[2]) з бази елементів Sync Architect.

^[1]PRC – Primary Reference Clock

^[2]SEC – Synchronous Equipment Clock

Однією з вагомих переваг Sync Architect є можливість моделювання роботи спроектованої мережі з метою виявлення проблемних ділянок (зокрема, в частині виникнення петель синхронізації) та внесення відповідних змін в структуру мережі та/або в налаштування окремих елементів. Останні версії програмного пакету Sync Architect адаптовано до змін, що відбулись в інфраструктурі телекомунікаційних мереж в результаті переходу на пакетні методи передавання та комутації. Зокрема, передбачено використання технології синхронного Ethernet (SyncE) замість традиційного передавання сигналів синхронізації по трактах SDH.

Застосування Sync Architect дозволяє оператору оптимізувати процеси планування та експлуатації мереж синхронізації, ефективно використовувати наявні ресурси і оперативно реагувати на зміни, що відбуваються в мережі. В сучасних умовах, коли структура телекомунікаційних мереж є дуже складною і різноманітною, використання подібних програм є особливо актуальним і корисним.

Слід відзначити позитивний досвід застосування програмного пакету Sync Architect в навчальному процесі на кафедрі телекомунікацій Інституту телекомунікаційних систем (ІТС) КПІ ім. Ігоря Сікорського. Протягом кількох років студенти успішно використовували Sync Architect під час виконання лабораторних та курсових робіт з навчальних дисциплін “Основи теорії мереж синхронізації та розповсюдження часу” і “Системи синхронізації та навігації” [2, 3]. Це дозволило спростити процес розробки схеми синхронізації відповідно до завдання і уникнути можливих помилок. Широкі можливості програмного пакету Sync Architect в частині візуалізації структури та елементів проектованої мережі, а також формування звітності (журнал подій, звіти про конфігурацію окремих елементів мережі тощо) сприяли кращому засвоєнню студентами учбового матеріалу та дозволили набути практичного досвіду роботи з сучасними інструментами проектування мереж.

Література

1. Тріска Н.Р. Актуальні завдання підготовки телекомунікаційних мереж до впровадження стандарту 5G. – Тринадцята Міжнародна науково-технічна конференція “Перспективи телекомунікацій” (ПТ-2019), 15-19 квітня 2019 р. Матеріали конференції. – ІТС НТУУ “КПІ”. – С. 131-133.
3. М.Л. Бірюков, Н.Р. Тріска Завдання та методичні вказівки для виконання курсової роботи з дисципліни “Основи теорії мереж синхронізації та розповсюдження часу”. – Кафедра телекомунікацій ІТС НТУУ “КПІ”. – К., 2012. – 25 с.
2. Тріска Н.Р. Методичні вказівки до виконання лабораторних робіт з навчальної дисципліни “Системи синхронізації та навігації”. – Кафедра телекомунікацій ІТС НТУУ “КПІ”. – К., 2016. – 102 с.

ИСПОЛЬЗОВАНИЕ ПУАССОНОВСКОЙ МОДЕЛИ ДЛЯ АНАЛИЗА ПРОСКАЛЬЗЫВАНИЯ В ПЛЕЗИОХРОННОМ СОЕДИНЕНИИ

Бирюков Н.Л., Триска Н.Р.

Институт телекоммуникационных систем КПИ им. Игоря Сикорского

E-mail: nlbir2@ukr.net, ntriska@ukr.net

The slip analysis in the plesiochronous connection using Poisson model

The probabilistic analysis of slips in plesiochronous connections using the Poisson model is presented. The simulation of slip dynamics in the single and multiple connections in plesiochronous networks was performed.

Существует несколько подходов к оцениванию проскальзывания как в одиночном соединении, так и в цепи последовательных соединений. Самый распространенный подход использует принцип “наихудшего случая”, т.е. оценку проскальзывания при экстремальном отклонении частот. При этом предполагается, что сравниваемые частоты максимально удалены друг от друга и находятся на противоположных границах диапазона $[f_0 - \Delta f, f_0 + \Delta f]$ допустимых отклонений частоты Δf от номинального значения f_0 [1, 2]. Другими словами, если $f_1 = f_0 - \Delta f$, а $f_2 = f_0 + \Delta f$, то $f_2 - f_1 = 2\Delta f$, что для нормированной частоты $y = \Delta f / f_0$ равно $2y$.

Второй – вероятностный подход предполагает случайный порядок размещения частот в пределах допустимого диапазона [2]. Если сравниваемые частоты могут с равной вероятностью находиться на любых позициях в диапазоне $[-1, +1]$, то нормированный модуль разности распределен по закону:

$$p_{\xi}(|y|) = 1 - \frac{1}{2}y, \quad y \in [0, 2] \quad (1)$$

В предположении нормального распределения двух частот на интервале $[-1, 1]$ ^[1], абсолютная величина их разности равна:

$$p_{\xi}(|y|) = \sqrt{\frac{2}{\pi}} \frac{1}{\sigma} e^{-\frac{y^2}{2\sigma^2}}, \quad y \in [0, 2] \quad (2)$$

Приведенные выше подходы позволяют получать оценки при экстремальном отклонении частот или значения, ожидаемые в среднем либо при заданной вероятности проскальзывания в соединении с двумя независимыми генераторами одинаковой точности, то есть в плезиохронном режиме. Однако при непосредственном распространении этих подходов на последовательно соединенные линии следует внести некоторые уточнения. Например, можно распространить “экстремальный” подход, разделив ожидаемое время проскальзывания на одном участке на количество участков в соединении. Однако моделирование “экстремального” случая показывает, что вероятность нахождения частот на противоположных границах диапазона равна вероятности того, что их значения совпадают [2]. Как следствие, среднее число экстремальных отклонений сокращается в два раза.

^[1]Принято, что нормированный диапазон $2 \cong 2\Delta f \approx 6\sigma$

Моделирование разбросов частот по участкам составного соединения и разброса при последовательной организации составного соединения, показывает характерные отличия между ними [2]. Отличие заключается в том, что в первом случае интервал между проскальзыванием меньше и монотонно убывает. Во втором случае интервал времени между проскальзыванием в среднем оказывается больше, чем в первом случае, а также наблюдается увеличение интервала проскальзывания на двух последовательных участках из-за того, что одна и та же частота участвует в двух соединениях – входящем и исходящем. Оценивание проводилось по абсолютной величине расхождения частот на каждом участке с последующим суммированием абсолютных расхождений. В качестве рабочей гипотезы учтено то, что знак отклонения частоты может совпадать или отличаться, что в последовательном соединении может приводить к снижению вероятности проскальзывания и увеличению временного интервала между проскальзыванием. Если знак совпадает, то расстояние между частотами δ не превышает половину допустимого диапазона $\delta \leq \Delta f$, при различных знаках отклонения частот в соединении набег фазы также имеют противоположные знаки и компенсируют друг друга, снижая вероятность проскальзывания.

Цель настоящей работы заключается в уточнении динамики проскальзывания (методики расчета) в составном соединении. Поток любых редких событий можно представить Пуассоновским потоком [3]. Результаты моделирования [2] показывают, что поток интервалов проскальзывания циклов имеет экспоненциальное распределение, что также согласуется с данными [4] об экспоненциальном распределении времени проскальзывания ФАПЧ. В данной работе представлены результаты использования модели Пуассоновского потока при оценивании проскальзывания в соединении из нескольких последовательно соединенных центров коммутации (рис. 1).

Проскальзывания возникают через интервалы времени t_{sl} , в течение которых сдвиг фаз сигналов записи и считывания, обусловленный разностью частот, превышает некоторую допустимую величину x_{lim} . Представив нормированную разность частот как δy_0 , а допустимую величину сдвига – как x_{lim} , можно записать условие возникновения проскальзывания в виде:

$$x_{lim}(t) \leq t \cdot \delta y_0 \quad (3)$$

Разность частот δy_0 и фаза расхождения частот записи и считывания в общем случае представляют случайную величину. Например, при “экстремальном” оценивании (когда $\delta = 2y_0$) такие отклонения при сравнении частот с нормальным или равномерным распределением возникают с вероятностью порядка $\sim 10^{-5}$. Значения δ для распределений (1) и (2) с равномерным (UD) и нормальным (ND) распределением частот приведены в таблице 1. Номинальные нормированные величины точности $y_0 = 10^{-\nu}$ в телекоммуникационных приложениях находятся в диапазоне $10^{-6} \div 10^{-12}$. Допустимое расхождение фаз, в зависимости от приложений, может варьироваться от примерно половины единичного интервала, нескольких бит или байт в указателях SDH, до половины емкости буферной памяти (БЗУ) и, например, в ЦАТС составляет 125 мкс. Из (3) получаем ожидаемую величину интервала проскальзывания $t_{sl} = x_{lim}/\delta y_0$, при

этом средняя интенсивность проскальзывания равна:

$$\lambda = \delta \cdot 10^{-\nu} / x_{\text{lim}}, \quad (4)$$

где значение δ зависит от принятых предположений, приведенных в таблице 1. Например, при равномерном распределении $\delta=0,67$, и интенсивность проскальзывания почти в 3 раза меньше, чем в “худшем случае”, а при нормальном распределении – в 5 раз меньше. Графики на рис. 2 и 3 иллюстрируют распределение проскальзывания при $\nu=11$ и $x_{\text{lim}}=125$ мкс (варианты экстремального оценивания, |UD + UD| и |ND + ND|) на одном и нескольких участках соединения. Использование Пуассоновской модели в случае пакетной передачи оставлено для дальнейшего исследования.

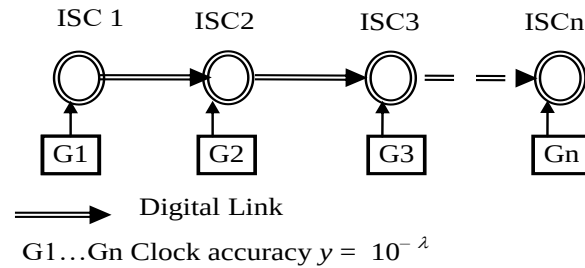


Таблица 1.

Параметр	δ		
	ND + ND	UD + UD	Extreme
Среднее $\mu_1 =$	≈ 0.38	≈ 0.67	2
Стандарт $\sigma =$	≈ 0.28	≈ 0.47	–
$\lambda \sim$	$0.4 \cdot 10^{-\nu}$	$0.7 \cdot 10^{-\nu}$	$2 \cdot 10^{-\nu}$

Рис. 1. Гипотетическое соединение n коммутационных центров (ISC).

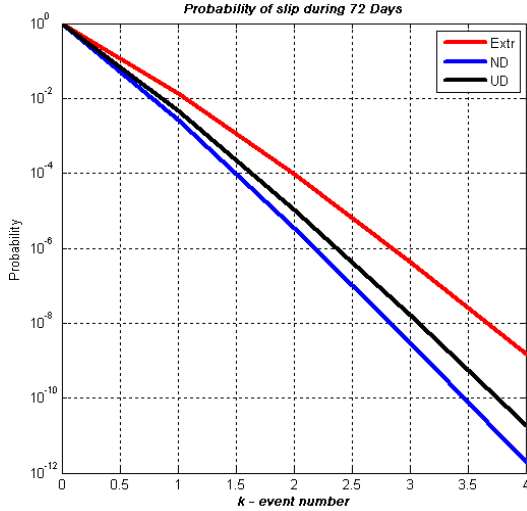


Рис. 2. Вероятность проскальзывания в течение 72 дней на 1 участке при различных интенсивностях Пуассоновского потока.

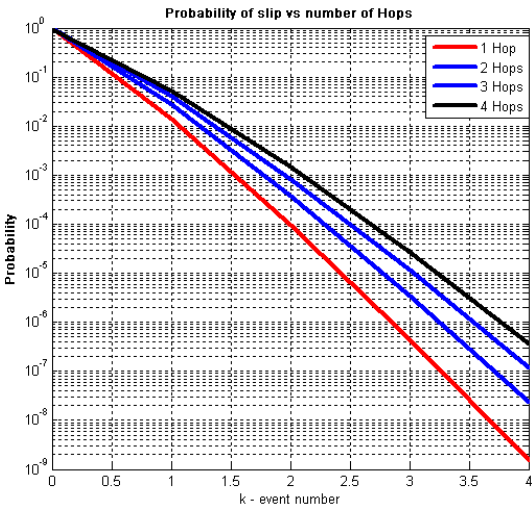


Рис. 3. Зависимость вероятности проскальзывания от числа последовательно соединенных участков и при различных интенсивностях Пуассоновского потока.

Литература

1. Бирюков Н.Л., Триска Н.Р. Анализ проскальзывания в плезиохронной сети. Т-Comm: Телекоммуникации и транспорт, 2016. – Том 10, №2. – С. 19-24.
2. Бирюков Н.Л., Триска Н.Р., Шварц М.Л. Режимы синхронизации и качественные показатели передачи. – Системы синхронизации, формирования и обработки сигналов. – № 2-2019. – С.52-57.
3. Тихонов В.И. Статистическая радиотехника. – 2-е издание переработанное и дополненное. – М.: Радио и связь, 1982. – 624 с.
4. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. 2-е изд.: Пер. с англ. – М: Издательский дом “Вильямс”, 2003. – 1104 с.: ил.

КОНВЕЄРНА ОБРОБКА ДАНИХ В КОМУТАТОРАХ МЕРЕЖІ SDN**¹Атаманчук М.В., ²Романов А.О.**¹*Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського¹*²*Факультет аеронавігації, електроніки та телекомунікації НАУ²**E-mail: atamanchuk14kolya@gmail.com, anton3329@gmail.com***Conveyor data processing in SDN switches**

One of the features of package processing in SDN network elements is the use of flow tables. Furthermore, the treatment of incoming flows is carried out by sequentially checking the address part of packages with the information recorded in the flow tables. In the work it is proposed to reduce the number of steps in selecting the direction of future packet forwarding.

Сучасні інформаційні технології висувають все більші вимоги до гнучкості і масштабованості телекомунікаційних мереж. Саме завдяки таким вимогам людство прийшло до нової технології комп'ютерних мереж, SDN. Програмно -конфігуровані мережі відрізняються від інших тим, що мають власний мозок, який контролює всю структуру мережі та забезпечує доступ до кожного з її елементів. Таким мозком є контролер. Основним елементом мережі, який працює під керівництвом контролера є комутатор. Взаємодія комутатора і контролера в SDN йде на основі протоколу OpenFlow. При цьому, комутатори повинні вміти відрізнити різні види трафіку: спам, сигнальний, данні та інші.

Таке ускладнення системи управління надає ряд переваг [1]:

- гнучке управління мережами та мережевими ресурсами;
- швидке впровадження нових сервісів;
- незалежність від виробників мережевого обладнання;
- широкі можливості забезпечення мобільності користувачів;
- швидке впровадження нових технологій.

Розглянемо особливості роботи комутатора SDN на основі протоколу OpenFlow в процесі обслуговування пакетів. Функціонально комутатор OpenFlow має одну або декілька таблиць потоків і групових таблиць. Вони, при необхідності, забезпечують пошук і пересилку пакетів, з одного або декількох каналів OpenFlow на зовнішній контролер. Комутатор зв'язується з контролером, і контролер управляє комутатором по протоколу комутатора OpenFlow. Кожна таблиця потоків в комутаторі містить набір записів потоків. Кожна запис потоку складається з полів збігу, лічильників і набору інструкцій, які повинні застосовуватися до пакетів. Обслуговування пакету починається з зіставлення пакету з першою таблицею потоків і може тривати до додаткових таблиць потоків конвеєра. Записи відповідають порядку пріоритету. Якщо відповідний запис знайдений, виконуються інструкції, пов'язані з конкретним записом потоку. Якщо в таблиці потоків збіг не знайдено, результат залежить від конфігурації записи потоку пропущених таблиць.

Комутатор OpenFlow повинен мати хоча б одну вхідну таблицю потоків. Таблиці потоків комутатора OpenFlow нумеруються в тому порядку, в якому вони можуть переглядатися пакетами, починаючи з 0. Конвеєр OpenFlow очікує, що зіставлення з обладнанням є узгодженим, і що конвеєр OpenFlow поводитиметься узгоджено.

Таблиця потоків складається із записів потоків. Запис потоку складається з: головних полів, лічильників, дії. Кожен запис таблиці потоків містить поля зіставлення з пакетами. Вони складаються з вхідного порту і заголовків пакетів. Запис таблиці потоків ідентифікується по її полях і пріоритетам зіставлення: поля збігів і пріоритет, взяті разом, ідентифікують унікальний запис в конкретній таблиці потоків. Записи потоку обробляються по порядку, і як тільки збіг знайдено, подальші спроби зіставлення з цією таблицею потоку не робляться.[3]

Можливі такі ситуації:

- Повна відповідність – це означає, що підтримуються всі поля відповідності.
- Відповідність другого рівня – це означає, що підтримуються тільки поля заголовка другого рівня.
- Відповідність третього рівня – це означає, що підтримуються тільки поля заголовка третього рівня.[4]

Запис потоку, яка не підлягає жодному із полів (всі поля пропущені) і має пріоритет рівний 0, називається записом потоку таблиці пропусків (якщо жодна запис потоку не збігається). У цьому випадку пакет пересилається на контролер.

Іншим типом елементів записи в таблиці є «дія» (action). Action визначає яким чином потрібно вести обробку пакетів потоку.

Нарешті, останнім типом елементів таблиці є елементи, які містять різну статистику - тривалість потоку, число отриманих та переданих пакетів і т.п. Після отримання пакета комутатор OpenFlow виконує певні функції. Поля заголовка, що використовуються для пошуку в таблиці, залежать від типу пакета.

Таким чином, таблицю потоків можливо представити у вигляді рис.1.



Рис.1. Типи елементів в таблиці потоків.

При отриманні першого пакету комутатор запускається і виконує пошук в першій таблиці потоків. Потім в другий і далі йде в конвеєр обробки. При необхідності може виконувати пошук в таблицях в інших потоків.[3]

Однак роботу комутатора можна організувати іншим чином. Комутатор можна налаштувати так, щоб пакет проходив перевірку тільки до першого співпадіння. Такий підхід зменшить час передачі пакету в мережі, та дозволить заощаджувати кошти на об'ємах пам'яті комутатора а також потужності процесора для опрацювання пакетів. Крім того, буде можливим прийняти однозначне рішення для подальшої обробки пакетів.

В такому разі робота комутатора буде здійснюватися таким чином. Комутатор запускається з виконання пошуку в першій таблиці потоків співпадіння із інформацією з пакету. Якщо співпадіння не знайдено, пакет проходить конвеєрну перевірку з іншими таблицями до тих пір, поки не буде знайдено першого співпадіння. Якщо жодне поле з пакету не співпадає з таблицею комутації, то пакет пересилається на контролер. Якщо співпадіння знайдено, то пакет передається до наступного комутатору.

Таким чином, в роботі розглянуто принцип конвеєрної обробки пакетів в комутаторі мережі SDN на основі протоколу OpenFlow. Визначено що, як правило, пакет який поступив на комутатор, повинен пройти через всі таблиці комутації та знайти співпадіння для кожного свого запису. Якщо всі поля пакету співпадають із всіма полями з таблиці комутації, то такий пакет означає повну відповідність і передається до наступного елементу мережі. Якщо не всі поля з пакету співпадають з полями із таблиці комутації, а такому разі до пакету застосовуються певні інструкції, записані в полі «дія». Якщо поля в пакеті взагалі не співпадають з полями із таблиці комутації, то пакет передається до контролеру.

В роботі запропоновано змінити принцип роботи комутатору таким чином, щоб співставлення проходило до першого співпадіння. Якщо є хоча б одне співпадіння в полях пакету з полями таблиці комутації, то зразу передавати пакет до іншого елементу мережі. Такий підхід дозволяє зменшити час обробки пакету в комутаторі та зменшити невизначеності при прийнятті рішення.

Література

1. Романов О.І., Діденко І.В. Особливості взаємодії контролера і мережевих пристроїв в мережах SDN з використанням протоколу OPENFLOW. Матеріали одинадцятої МНТК «Проблеми телекомунікацій», Київ, 2017 р. С 142-145.
2. О.І. Романов, М.М. Нестеренко, В.Б. Маньківський. Застосування регресійної моделі коефіцієнта використання каналів для формування плану розподілу навантаження в мережі. Науково-технічний журнал Вісник НТУУ "КПІ". Серія Радіотехніка, Радіоапаратобудування №67, 2016 с.34-42.
3. "OpenFlow Specification 1.5.1" - Open Networking Foundation, March 15, 2015.
4. https://myweb.ntut.edu.tw/~phtseng/SDN/OpenFlow_v2.pdf.
5. <https://www.google.ch/patents/WO2014192005A1?cl=en>.

ЗАХИЩЕНІСТЬ ІНФОРМАЦІЙНИХ СИСТЕМ ПРИ ВИКОРИСТАННІ ТЕХНОЛОГІЙ ВІРТУАЛІЗАЦІЇ

¹Романов О.І., ¹Нестеренко М.М., ²Фесьоха Н.О.

¹ Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського

² Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут

E- mail: a_i_romanov@gmail.com, nikolaiy.nesterenko@gmail.com, nadya_viti@i.ua

Protection of information systems in the use of virtualization technologies

Information technology is rapidly evolving, bringing to life many useful tools for work, science. One of the most promising technologies in the computer world is virtualization.

Інформаційні технології стрімко розвиваються, приносячи в повсякденність безліч корисних засобів для роботи, науки. Однією з перспективних технологій в комп'ютерному світі є віртуалізація.

Віртуалізація в інформаційних технологіях (ІТ) - процес подання набору обчислювальних ресурсів або сутностей, який дає певні переваги перед звичайною конфігурацією.

Аналітична компанія *Gartner* в своєму щорічному списку топ-10 стратегічних технологій 2019 виділяє підвищене питання інформаційної безпеки (ІБ).

Отже постає питання: як впливають технології віртуалізації на ІБ. Підвищується, знижується або залишається на попередньому рівні. Існування різних видів віртуалізації не дозволяє дати однозначну відповідь.

Віртуалізація комп'ютера - найбільш поширений вид віртуалізації. Виділяють технології програмної і апаратної віртуалізації. Програмна віртуалізація несе в собі ряд особливостей, що створюють серйозні проблеми ІБ: гіпервізор і хостова ОС представляють єдину точку відмови; реалізація гіпервізора у вигляді програмного модуля більш вразлива до атак, ніж апаратно-програмна реалізація; за технологією *Trusted Platform Module (TPM)* відомі рішення з програмною віртуалізації не забезпечені захистом на апаратному рівні.

Більш сучасні технології апаратної віртуалізації вирішують ряд зазначених проблем ІБ. Для підвищення захищеності компанія *Intel* впровадила в одному зі своїх чіпсетів технологію безпеки *LaGrande / TXT*, що використовує специфікацію *TPM 1.2*. Дана технологія дозволяє контролювати цілісність програмно-апаратного середовища комп'ютера. Аналогічні механізми безпеки забезпечує технологія *AMD-V*, в якій реалізований спеціальний захищений режим запуску монітора віртуальних машин.

Віртуалізація мереж являє собою перетворення елементарних мережевих ресурсів типу фрейму, пакета, сесії і управління ними. При цьому можуть використовуватися каналний, мережевий, транспортний і сесійний рівні моделі OSI.

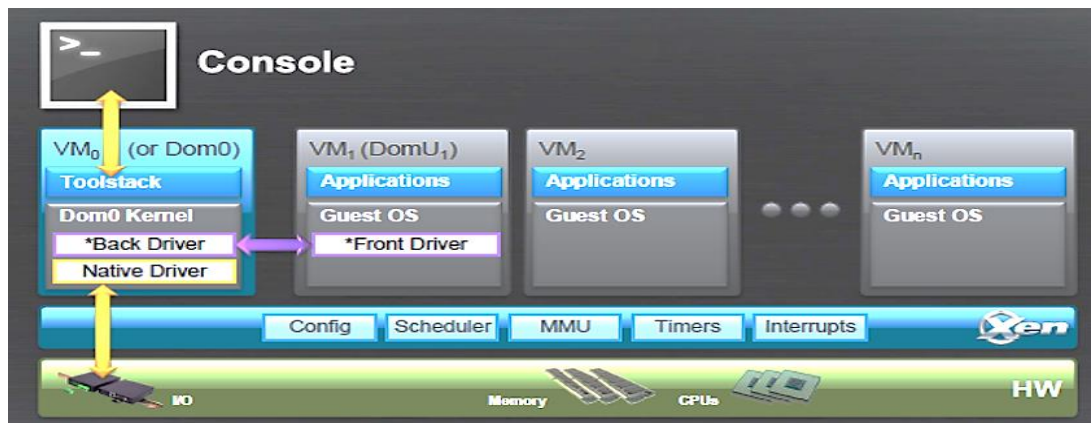


Рис. 1. Гіпервізор
Xen типу 1.

Віртуалізація мереж можлива за технологією віртуальної приватної мережі (ВПМ) і за технологією віртуальної локальної обчислювальної мережі (ВЛВС). ВПМ має глобальний характер застосування, так як працює на мережевому рівні, в ВЛВС - тільки локальний. Основними цілями віртуалізації мереж є: поділ і управління потоками інформації, мережева ізоляція, сегментування мережі, а також захист інформації при її передачі по мережі.

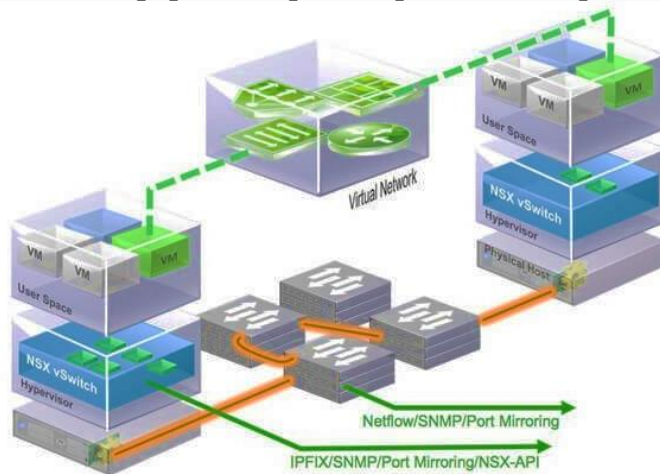


Рис. 2. Віртуалізація мережі.

При віртуалізації додатку формується кілька незалежно працюючих додатків (з контекстами) або його користувальницькі представлення (термінальні сесії, профілі користувачів). Віртуалізація додатків має мету: відокремити додатки від операційної системи, зробити їх мобільними і

надати можливість для їх виконання в різних середовищах. Віртуалізація представлень - підхід, при якому додаток виконується на віддаленому сервері, а його користувальницький інтерфейс відображається локально. Віртуалізація представлень широко використовується в сучасних додатках для управління клієнтськими додатками і захисту конфіденційних даних.

Віртуалізація мереж на базі загальноприйнятих (*IPSec*, *SSL*) і приватних протоколів - склала, самостійний напрям мережевої безпеки. Віртуалізація представлень за допомогою термінальної сесії - доцільний метод ізоляції сервера додатків і робочої станції користувача. Ізоляція користувача і сервера важлива при їх локалізації в двох зонах, протилежних за умовами ІБ. При термінальній сесії на сервер передаються тільки коди натиснутих клавіш робочої станції, а з сервера - растри призначеного для користувача інтерфейсу. Важливо, що між сервером і робочою станцією немає обміну програмним кодом, що виключає ризик передачі шкідливих програм.

Ізоляцію бази даних та процесів між віртуальними машинами забезпечують нові продукти компанії *IBM*, *Intel*, *Microsoft*, *AMD*, *Citrix (Zen)*, *VMware*. Гарантована ізоляція дає можливість їх використання для розділення операційних середовищ за рівнем конфіденційності інформації, обраних в системі.

Технологія апаратної віртуалізації, що використовує модуль *TPM* і специфікації *TCG* для реалізації довіреного середовища, дозволяє створювати безпечні розділи з перевіркою ідентичності і цілісності віртуальної машини і усіх задіяних в ній програмно-апаратних компонент. Поки що тільки компанії *Parallels* і *Microsoft* поставляють на ринок продукти віртуалізації, що застосовують ці технології захисту. Компанія *Parallels* працює над використанням *Intel VT-x* і *TXT* для створення монітора віртуальних машин з гарантованим захистом від вірусів. Компанія *Microsoft* використовує технологію апаратного захисту у рамках *Windows Server 2008* і *Hyper-V Server*.

Компанії *Microsoft* і *Citrix* застосовують технологію апаратної віртуалізації *Intel* для контролю середовища користувача, завантаження образів ОС і додатків з корпоративного сервера. Усі необхідні застосування і ОС знаходяться на одному сервері - їх легко контролювати і захищати. При цьому реалізується контроль призначеного для користувача доступу до додатків за допомогою регульованого переліку додатків для конкретного облікового запису.

Одним з головних напрямів застосування технології віртуалізації в завданнях ІБ є забезпечення доступності інформації і безперервності процесів (*BCP*, *DRP*). Данні задачі вирішуються за допомогою віртуалізації серверів і систем зберігання даних. Віртуалізація економить значні інвестиції в порівнянні з фізичним дублюванням і резервуванням устаткування.

Незважаючи на нові можливості у сфері ІБ, застосування технології віртуалізації несе в собі нові загрози.

Досить порівняти надійність ізоляції віртуальних машин з варіантом фізично ізольованих комп'ютерів. Навіть у нових технологіях апаратної віртуалізації частина механізму віртуалізації реалізується програмним забезпеченням гіпервізора. Незважаючи на оптимізацію об'єму коду гіпервізора і пильну увагу розробників до усунення можливих вразливостей, існує вірогідність наявності прихованих або функціональних вразливостей гіпервізора і можливості проведення проти нього атаки.

Знижує захищеність і простота переносимості віртуальних систем на інші фізичні платформи, використання віртуальних машин в архітектурі "хмарних обчислень".

Системи з віртуалізацією комп'ютерів мають одну точку відмови - ОС і ПО віртуалізації хост-комп'ютера. Такий недолік не дозволяє використати програмну віртуалізацію в завданнях забезпечення безперервності процесів, там, де потрібна висока готовність і доступність інформації. Важливою особливістю застосування технології віртуалізації вважається розробка життєвого циклу інформації, що захищається, при міграції віртуальних хостів і балансування навантаження. У останніх технологічних рішеннях міграція віртуальних машин і даних залишається однією з базових функцій. Нерегульована міграція даних обмеженого доступу недопустима, оскільки здатна привести до порушень її конфіденційності, цілісності і доступності, а в цілому - до зростання ризиків ІБ.

Отже: сама по собі віртуалізація ІТ-обладнання (процесорних систем, комп'ютерів, систем зберігання даних і тому подібне), а також програмних застосувань і ресурсів не є механізмом ІБ. Віртуалізація мережевого ресурсу (*IP*-пакет), протоколу (*IPSec*, *SSL*), що включає криптографічні методи захисту, вважається механізмом забезпечення безпеки, який дозволяє створювати нові технології мережевого захисту. За винятком віртуалізації представлень, технологія

віртуалізації додатків не призводить до підвищення рівня ІБ, оскільки віртуалізовані застосування не мають гарантованої взаємної ізоляції по міграції програмного коду. Віртуалізація представлень - наприклад, режим термінального доступу - забезпечує межу між клієнтом і сервером, що захищає від проникнення шкідливого програмного коду.

Іншим аспектом ІБ є гарантована ізоляція процесів і цих віртуальних машин один від одного. Проте гарантія ізоляції віртуальних машин за даними не може бути стовідсотковою, оскільки пов'язана з потенційними вразливостями гіпервізора. В порівнянні з фізично ізольованими хостами (відсутність віртуалізації) рівень ризиків ІБ вищий при використанні технологій апаратної віртуалізації і істотно вищий - при реалізації технологій програмної віртуалізації. Для зниження ризиків ІБ у рамках застосування апаратної віртуалізації повинна працювати технологія апаратного захисту на основі модуля *TPM* і специфікації *TCG*.

Використання технологій віртуалізації в ІС вимагає розробки регламенту по захисту інформації, залученої в процеси міграції віртуальних машин. Рекомендується застосування технології віртуалізації для забезпечення безперервності процесів (*BCP*, *DRP*) за рахунок резервування обладнання і програмного забезпечення їх віртуальними аналогами. Для вирішення подібних завдань найбільшою мірою підходить технологія апаратної віртуалізації.

Література

1. Романов О.І., Нестеренко М.М., Фесьоха Н.О. Віртуалізація як спосіб організації інфраструктури інформаційно-телекомунікаційних мереж// Збірник матеріалів Міжнародно науково-технічної конференції «Перспективи телекомунікацій»/Збірник тез конференції (ISSN print 2663-502X). К.: КПІ ім. Ігоря Сікорського, 2019
2. Y. Li, W. Li, and C. Jiang, "A Survey of Virtual Machine System: Current Technology and Future Trends", in Proceedings of the Third International Symposium on Electronic Commerce and Security, 2010.
3. J. E. Smith, and R. Nair, "The Architecture of Virtual Machines", Computer, vol. 38, No. 5, pp. 32-38, 2005.
4. S. Nanda, and T. Chiueh, "A Survey on Virtualization Technologies", Experimental Computer Systems Lab, SUNY Stony Brook, SUNY RPE Report TR-179, 2005.
5. О. С. Головня, "Систематизація технологій віртуалізації", Інформаційні технології в освіті, № 12, с. 127-133, 2012.
6. О. С. Головня, Технології віртуалізації у навчанні операційних систем бакалаврів інформатики: Методичні рекомендації для викладачів вищ. навч. закл.. Житомир: Рута, 2017, с. 15-20.
7. О. S. Holovnia, "Criteria for selecting virtualization software in teaching unix-like operating systems", Information technologies in education, No. 24, p. 119-133, 2015.
8. F. Giraldeau, M. R. Dagenais, and H. Boucheneb, "Teaching operating systems concepts with execution visualization", in 121st ASEE Annual Conference and Exposition, Indianapolis, IN, USA, 2014.
9. A. Garmpis, and N. Gouvatsos, "Innovative teaching methods in Operating Systems: The Linux case", in Innovative approaches in Education: Design and Networking, 2012.
10. О гипервизорах, виртуализации систем и о том, как это работает в облачной среде. [Электронный ресурс] - Режим доступа:
<https://www.ibm.com/developerworks/ru/library/cl-hypervisorcompare>.

Секція 4. Безпроводові телекомунікаційні системи
та технології, системи 5G, Інтернет речей

УДК 621.396.1

**РЕГУЛЮВАННЯ ВИКОРИСТАННЯ БЕЗПІЛОТНИХ
ЛІТАЛЬНИХ АПАРАТІВ ДЛЯ МОНІТОРИНГУ ОБ'ЄКТІВ**

Кравчук І.М.

Інститут телекомунікаційних систем КПІ ім. І. Сікорського, Україна

E-mail: sakravchuk@ukr.net

Regulation of use of UAVs for monitoring objects

The formation of a system of legal regulation of actions for the management of unmanned aerial vehicles (UAVs), including the management of a swarm of drones, is presented.

Формування системи правового регулювання дій по керуванню безпілотних летальних апаратів (далі - БЛА), в тому числі і при керуванні рою дронів [1], базується на основних напрямках: використання повітряного простору щодо безпеки польотів, і безпеки об'єктів моніторингу; введення оперативних обмежень на польоти дронів; визначення адміністративно-правових процедур видачі дозволів на політ, ліцензій на збір даних та ін. Крім того, окремим напрямком правової регламентації є збір і обробка інформації про людей, яка становить їх персональні дані [2].

Необхідно зауважити, що на міжнародному рівні прийнято цивільні авіаційні правила, які забороняють БЛА літати над територією іншої держави без її дозволу [3]. Існують загальні правила використання БЛА, які діють в усіх країнах, а саме: завжди використовувати в полі зору, не вище допустимих норм, заборона польотів в зоні аеропортів, стратегічних об'єктів, а також не наближатися до людей та тварин.

На сьогодні в Європейському Союзі існує нормативно-правова база регулювання польотів БЛА: Про загальні правила в галузі цивільної авіації та створення Агентства з безпеки польотів Європейського союзу [4], Делегований Регламент Європейської Комісії «Про безпілотні літальні системи та операторів безпілотних літальних систем третіх країн». Новелою цих документів є визначення вимог, яким повинні відповідати БЛА, щоб їх можна було використовувати без необхідності отримання попереднього дозволу від органів влади [5]. Крім того, визначено поняття «unmanned aircraft» ('UA'), тобто «безпілотний літак», який визначено, як будь-який літак, який експлуатується або призначений для роботи автономно або для

дистанційного керування без пілота. П. 23 ст. 1 Повітряного кодексу України практично визначена така ж сутність терміну «безпілотне повітряне судно» - це таке повітряне судно, яке призначене для виконання польоту без пілота на борту, керування польотом якого і контроль за яким здійснюються за допомогою спеціальної станції керування, що розташована поза повітряним судном [6]. На сьогодні в Україні відбуваються спроби врегулювати правила застосування БЛА, прийнято ряд норм в цьому напрямку [7-9].

Відповідно до вимог пункту 4 розділу II Правил використання повітряного простору, польоти БЛА масою до 20 кг включно виконуються без подання заявок на використання повітряного простору, без отримання дозволів на використання повітряного простору, без інформування відповідних органів влади. Проте, таке використання можливо лише за умови дотримання наступних вимог, а саме якщо:

- польоти виконуються: без перетинання державного кордону України, поза межами встановлених заборон та обмежень використання повітряного простору; в межах прямої видимості (VLOS), при цьому швидкість польоту БЛА складає не більше 160 км/год.; не ближче 5 км від зовнішніх меж злітно-посадкових смуг аеродромів або не ближче 3 км від зовнішніх меж злітно-посадкової смуги вертодромів; не ближче 500 м від пілотованих повітряних суден;
- польоти не виконуються над: скупченням людей на відкритому просторі та над місцями щільної забудови; об'єктами (зонами), які визначені відповідними органами державної влади;
- якщо максимальна висота польоту не вище: 120 м над рівнем земної (водної) поверхні, 50 м над рівнем земної (водної) поверхні в межах спеціально встановлених зон, 50 м над статичними перешкодами на горизонтальній відстані не більше 100 м від таких перешкод, як відхилення від зазначених вище обмежень по висоті, на запит власника такого об'єкту. В інших випадках польоти безпілотного повітряного судна масою до 20 кг включно та усі без винятку польоти безпілотного повітряного судна масою більше 20 кг виконуються у межах спеціально встановлених зон та маршрутів з дотриманням вимог щодо подання заявок на використання повітряного простору, отримання дозволів та умов використання повітряного простору, інформування спеціальних органів в цій сфері [7-9].

Висновки. Прийняті норми лише фрагментарно урегульовують механізм використання БЛА, спеціального нормативно-правового акту в Україні на теперішній час не прийнято, який би врегулював питання сертифікації, атестації операторів, а також інтеграції в сферу управління повітряного руху, актуальним також залишається врегулювання питання використання здобутої інформації під час моніторингу об'єктів [2, 10].

Література

1. Кравчук С.О., Кравчук І.М. Підходи та стратегії щодо колективного керування роєм дронів. Збірник матеріалів Міжнародної науково-технічної конференції «ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ» (ПРОБЛЕМИ ТЕЛЕКОМУНІКАЦІЙ), 2019.
2. Баранов О.А. Інтернет речей : теоретико-методологічні основи правового регулювання. Т 1 : Сфери застосування, ризики і бар'єри, проблеми правового регулювання : монографія. Наук.-дослід. ін-т інформатики і права НАПрН України. 2-ге вид. Харків : Право, 2018. 344 с.
3. Ковтюх Н. П., Адміністративно-правове регулювання використання безпілотних літальних апаратів у Європейському Союзі. Актуальні проблеми вітчизняної юриспруденції № 3. 2019, С. 87-90.
4. REGULATION (EU) 2018/1139 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 4 July 2018 On common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No. 2111/2005, (EC) No. 1008/2008, (EU) No. 996/2010, (EU) No. 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No. 552/2004 and (EC) No. 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No. 3922/91. URL: <http://data.europa.eu/eli/reg/2018/1139/oj>.
5. COMMISSION DELEGATED REGULATION (EU) .../... of 12.3.2019 On unmanned aircraft systems and on third-country operators of unmanned aircraft systems. URL: https://ec.europa.eu/transport/sites/transport/files/legislation/c20191821-drones_en.pdf.
6. Повітряний кодекс України : Закон України від 19 травня 2011 року № 3393-VI. URL: <https://zakon.rada.gov.ua/laws/show/3393-17>.
7. Про затвердження Положення про використання повітряного простору України : Постанова Кабінету міністрів України від 6 грудня 2017 р. № 954. URL: <https://zakon.rada.gov.ua/laws/show/954-2017-%D0%BF>.
8. Про затвердження Авіаційних правил України «Правила використання повітряного простору України» : Наказ Державіаслужби України та Міністерства Оборони України від 01 травня 2018 р. № 430/210. URL: <https://zakon.rada.gov.ua/laws/show/z1056-18>.
9. Про схвалення Національної транспортної стратегії України на період до 2030 року : Розпорядження Кабінету міністрів України від 30 травня 2018 р. № 430-р. URL: <https://zakon.rada.gov.ua/laws/show/430-2018-%D1%80>.
10. Бакутін Є.І. Напрями вдосконалення законодавчого регулювання використання безпілотних літальних апаратів (БПЛА) в діяльності Національної поліції України. Держава і право : зб. наук. праць. Юрид. і політ. науки. 2017. Вип. 77. С. 307-320.

АЛГОРИТМ ВИБОРУ ДОПОМІЖНИХ ВУЗЛІВ ДЛЯ БЕЗПРОВОДОВОЇ КООПЕРАТИВНОЇ РЕТРАНСЛЯЦІЇ З ПЕРЕХОПЛЮВАЧЕМ

Афанасьєва Л. О.

Інститут телекомунікаційних систем КПІ ім.Ігоря Сікорського, Україна

E-mail: liana.afanasyeva@gmail.com

Selection algorithm of helper nodes in wireless cooperative relaying with eavesdropper

Due to broadcasting nature of wireless channel, information privacy is exposed to be undesirable overheard. Therefore, wireless network implementation feature requires a specific approach to ensuring the security. This paper provides an overview of the cooperative relaying with eavesdropper scheme. This paper provides an overview jamming technique that produce an artificial interference at the eavesdropper node in order to reduce the capacity of the link.

Конфіденційності інформації в безпроводових мережах приділяється значна увага через широкомовну природу безпроводового середовища, що дозволяє всім користувачам в зоні покриття передачі підслуховувати вихідне повідомлення [1]-[3]. Традиційно, захист інформації в безпроводових мережах реалізовується в основному на вищих рівнях з використанням криптографічних методів [4]-[5]. Однак, такі методи забезпечення секретності стають предметом збільшення потенційних атак, тому впровадження нових підходів, що реалізують безпеку каналів на фізичному рівні (РНУ) є актуальною задачею. В роботах [1] показано, що коли канал вузла, що підслуховує є погіршеною версією основного каналу, джерело і цільовий приймач можуть обмінюватися повідомленнями з безпечною ненульовою швидкістю, зберігаючи при цьому данні передачі від вузла, що підслуховує. Максимальна швидкість такої передачі від джерела до його цільового приймача називається безпечною швидкістю (secure rate), при якій ймовірність помилки декодування цільового приймача прагне до нуля, а ймовірність помилки для вузла, що підслуховує прагне до одиниці.

Розглядається системна модель кооперативної мережі джерело S - цільовий приймач D з одним перехоплювачем E (eavesdropper) і набором проміжних терміналів-ретрансляторів $S_R = \{1, 2, \dots, N\}$ з N вузлами (рис 1).

Проміжні вузли працюють в напівдуплексному режимі, отже, процес зв'язку здійснюється в два етапи по двом ортогональним каналах. Під час першої фази джерело S передає дані на цільової приймач D , і за рахунок широкомовного характеру передачі проміжні вузли ретрансляції R і перехоплювач E прослуховують передану інформацію.

Вузли генерації перешкод (jammer) J_1, J_2 працюють в «режимі перешкод», отже, не декодують вихідний сигнал, а застосовуються для генерації навмисних перешкод, щоб погіршити якість лінії зв'язку перехоплювача.

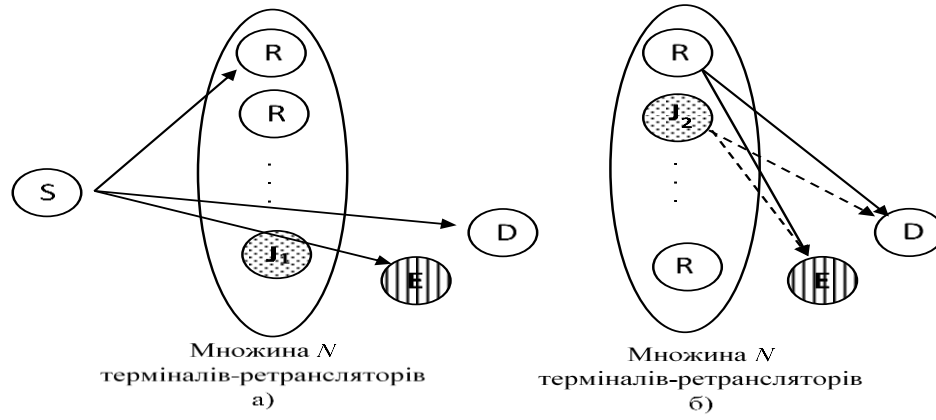


Рис.1. Схема кооперативної ретрансляції з перехоплювачем:
а) фаза широкомовлення, б) фаза кооперації.

Під час кооперативної фази, відповідно до схем безпеки вибирається проміжний вузол R , який успішно декодував вихідний сигнал з підмножини $C_d \in S_R$, для роботи в якості терміналу-ретранслятора та пересилає вихідне повідомлення на цільовий приймач D .

Алгоритм оптимальної схеми вибору R і J передбачає наявність набору значень певних параметрів для всіх ліній зв'язку, критерієм оптимальності є максимальне значення миттєвої пропускної здатності для набору декодування C_d .

Пропускна здатність при кооперативній ретрансляції з перехоплювачем може бути виражена в наступному вигляді:

$$C_S^{|C_d|}(R, J_1, J_2) = \left[\frac{1}{2} \log_2 \left(1 + \frac{\gamma_{S,D}}{1 + \gamma_{J_1,D}} + \frac{\gamma_{R,D}}{1 + \gamma_{J_2,D}} \right) - \frac{1}{2} \log_2 \left(1 + \frac{\gamma_{S,E}}{1 + \gamma_{J_1,E}} + \frac{\gamma_{R,E}}{1 + \gamma_{J_2,E}} \right) \right], \quad (1)$$

для $|C_d| > 0$,

де $R \in C_d, J_1 \in S_R, J_2 \in \{S_R - R^*\}, \gamma_{a,b}$ - миттєве відношення сигнал/шум (SNR) для лінії зв'язку $a \rightarrow b$, R^* - обраний термінал-ретранслятор. Вибір вузлів для передачі даних, які дозволять мінімізувати ймовірність збою зв'язку визначаються за наступними критеріями

$$(R^*, J_1^*, J_2^*) = \arg \max_{R \in C_d, J_1 \in S_R, J_2 \in \{S_R - R^*\}} \left\{ \frac{\gamma_{S,D} + \gamma_{R,D}}{\gamma_{J_1,D} + \gamma_{J_2,D}} \right\} \quad (2)$$

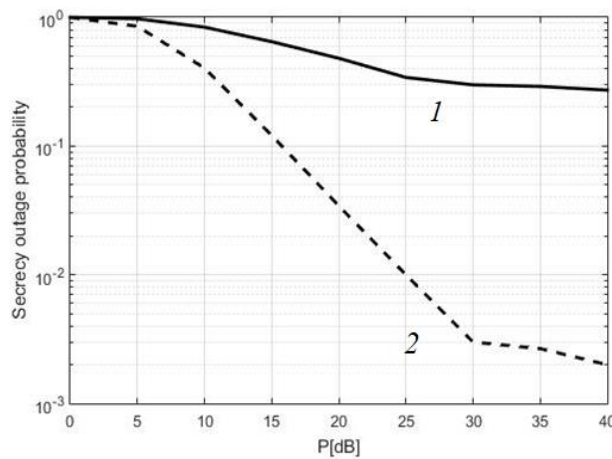
З рівняння (2) отримуємо

$$J_1^* = \arg \max_{J_1 \in S_R} \left\{ \frac{\gamma_{J_1,E}}{\gamma_{J_1,D}} \right\}, \quad (3)$$

$$R^* = \arg \max_{R \in C_d} \left\{ \frac{\gamma_{R,D}}{\gamma_{R,E}} \right\} \quad (4)$$

$$J_2^* = \arg \max_{J_2 \in \{S_R - R^*\}} \left\{ \frac{\gamma_{J_2,E}}{\gamma_{J_2,D}} \right\} \quad (5)$$

Розглянутий алгоритм передбачає вибір R по критерію максимального відношення $\gamma_{n,D}, \gamma_{n,E}$, в той час як для вузлів генерації перешкод J вибір ґрунтується на мінімальному значенні відношення $\gamma_{J,E}$ до $\gamma_{J,D}$. Отже, критерій вибору не залежить від порядку вибору і завжди будуть вибиратися різні термінали-ретрансляції.



1 - перехоплювач E знаходиться ближче до джерела S ,
2 - перехоплювач розташований ближче до цільового приймача D .

Рис. 2. Залежність вірогідності збою на лінії зв'язку від переданої потужності.

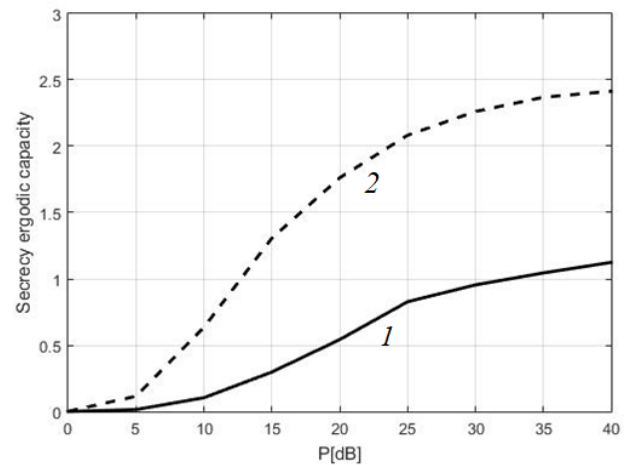


Рис. 3. Залежність пропускну здатності від переданої потужності.

Як можна бачити з графіків на рис.2 та рис.3, при розташуванні перехоплювача ближче джерела методи безперервного глушіння менш ефективні, а саме генерація перешкод забезпечує меншу ймовірність збою зв'язку та забезпечується краща продуктивність системи зв'язку при наявності шумів для випадку розташування J біля D .

Література

1. Silva E. D., Santos A. L. D., Albini L. C. P., Lima M. Identity based key management in mobile ad hoc networks: techniques and applications// IEEE Wireless Commun. . –2008. – vol. 15. – pp. 46-52 (DOI: <https://doi.org/10.1109/MWC.2008.4653131>).
2. S. Kravchuk, L.Afanasieva Wireless cooperative relaying without maintaining a direct connection between the source and target receiver terminals// Information and Telecommunication Sciences. – No 2, pp. 5-11, 2019 (DOI: <https://doi.org/10.20535/2411-2976.22019.5-11>).
3. Афанасьєва Л.О., Кравчук С.О. Протокол адаптивної ретрансляції для кооперативних мереж// Матер. 13-ї міжнар. наук.-техн. конф. “Перспективи телекомунікацій”, 15-19 квітня 2019 р. – К.: КПІ ім. Ігоря Сікорського, 2019. – С. 192–195.
4. Zou Y, Zhu J, Wang X, Leung VCM Improving physical-layer security in wireless communications using diversity techniques//IEEE Netw. –2015. – No. 29(1). – 42–48.
5. Li J., Petropulu A.P., Weber S. On cooperative relaying schemes for wireless physical layer security// IEEE Trans. Signal Process. –2011. –No. 59(10). – pp. 4985–4997 (DOI: <https://doi.org/10.1109/TSP.2011.2159598>).

СИСТЕМИ МОБІЛЬНИХ ІНФОКОМУНІКАЦІЙ

Кравчук С.О.

*Інститут телекомунікаційних систем КПІ ім. І. Сікорського, Україна
E-mail:sakravchuk@ukr.net*

Mobile Infocommunication Systems

At present, mobile communication systems have emerged as mobility-enabled information and telecommunication systems, or mobile information systems. The latter work equally well with both wireless and wired user access networks and IoT.

Протягом багатьох років телекомунікаційні й інформаційні технології розглядалися як окремі напрямки, однак в останні десятиліття відбувалось їх безперервне зближення (конвергенція) і створення єдиних інфокомунікаційних (інформаційно-телекомунікаційних) технологій. Сам термін телекомунікації з'явився як спадкоємець застарілого терміну електрозв'язок і тому він повністю не відображає того факту, що комунікації зв'язку не тільки передають а й обробляють інформацію, сформовану засобами інформаційних технологій. Сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле, визначається терміном інформаційно-телекомунікаційні або інфокомунікаційні системи.

На даний час продовжується формування нових та модернізація традиційних способів поширення/передачі інформації та доступу до інформаційних ресурсів. Зокрема, ефективними інструментами сучасних інфокомунікаційних систем є мобільні технології, що дають змогу своїм користувачам (їх мобільним пристроям і застосуванням) водночас вільно рухатись і використовувати мобільні послуги. За підтримуваним рівнем мобільності (рухомості) інфокомунікаційні системи можуть бути: з частковою (переносні термінали), неповною (низька швидкість руху терміналу), і повною (з рухом терміналу до 300 км/год) мобільністю.

Важливою складовою інфокомунікацій стали стільникові системи мобільного (рухомого) зв'язку, що реалізують радіодоступ до користувацьких терміналів, під час якого кінцеве обладнання хоча б одного із користувачів може вільно переміщуватися в межах інфокомунікаційної мережі, зберігаючи єдиний унікальний ідентифікаційний номер мобільного терміналу користувача. Системи мобільного зв'язку пройшли досить довгий шлях розвитку від звичайних стільникових радіосистем користувацького доступу, головною метою яких було забезпечення голосового зв'язку із ТМЗК (телефонною мережею загального користування), до сучасних гетерогенних інфокомунікаційних систем з підтримкою мобільності, що надають конвергентні комунікаційні послуги передачі голосу і даних,

послуги міжмашинної взаємодії M2M (machine-to-machine) та послуги Інтернету речей IoT (Internet of Things).

Ранішні системи мобільного зв'язку (територіальної телефонії), головним чином, визначались реалізацією своєї системи радіодоступу. В якості центрального вузла (ядра) слугувала традиційна телефонна комутаційна система (по принципу дії комутації каналів) типу локальної автоматичної телефонної станції з декількома додатковими вузлами (надбудовами), які повинні були узгодити інтерфейси станції з каналами безпроводової мережі доступу до терміналів користувачів, та забезпечити підтримку мобільності цих терміналів. Таким чином, при вивченні ранніх систем мобільного зв'язку найбільше уваги приділялось реалізації безпроводових технологій та принципів функціонування мережі користувацького доступу в умовах можливих глибоких завмирань сигналів. Відповідно, вивчення таких систем мобільного зв'язку вимагало, перш за все, радіотехнічної підготовки.

Зростання кількості користувачів і сервісів з підтримкою необхідної якості обслуговування, збільшення зони обслуговування мережі одного оператора, а головне, поява технологій і систем з комутацією пакетів, призвели до суттєвого ускладнення базової мережі мобільного зв'язку та її вузлів, зростання функціональності та інтелектуалізації ядра мережі. Поступово базова мережа та принципи її функціонування стали більш вагомими ніж реалізація мережі радіодоступу. Не дивлячись на це, інтенсивний розвиток останньої весь час продовжується і є важливим.

Звідси, для вивчення систем мобільного зв'язку стала затребуваною більш інтегрована інформаційно-телекомунікаційна підготовка, особливо із знання мережних та інформаційних технологій.

На даний час системи мобільного зв'язку сформувались як інформаційно-телекомунікаційні системи із підтримкою мобільності, або – системи мобільних інфокомунікацій. Останні однаково ефективно працюють як із безпроводовою, так і з проводовою мережами користувацького доступу та IoT.

Вагомий внесок послуг мобільних інфокомунікацій, що надаються в Україні, наочно підтверджують показники, наведені за даними Державної служби статистики України (без ПДВ, без урахування тимчасово окупованої території Автономної Республіки Крим, м. Севастополя та частини тимчасово окупованих територій у Донецькій та Луганській областях). Так у 2018 р. доходи від надання послуг зв'язку склали 61 976 млн грн, з них доходи від надання телекомунікаційних послуг склали 91,1 %, а доходи від надання послуг поштового зв'язку та кур'єрських послуг всього – 8,9 %.

В структурі доходів від надання телекомунікаційних послуг у 2018 р. найбільшу частку склали рухомий (мобільний) зв'язок – 61,9 % та фіксований доступ до мережі Інтернет – 14,4%, сумарна частка яких у загальних доходах від надання телекомунікаційних послуг склала 76,3 % (рис. 1).

В структурі доходів від надання послуг рухомого (мобільного) зв'язку найбільші частки становлять: доходи від надання послуг голосової телефонії

– 41,9% та доступу до мережі Інтернет – 45,8%, сумарна частка яких становить 87,7% (рис. 2).

Згідно річного «Звіту про роботу Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації за 2018 р.» (nkrzi.gov.ua) за період з 2016 р. по 2018 р. спостерігалась стала тенденція до збільшення доходів від надання послуг рухомого (мобільного) зв'язку, так у 2018 р. вони збільшились на 11,1% у порівнянні з 2017 р. (рис. 3).

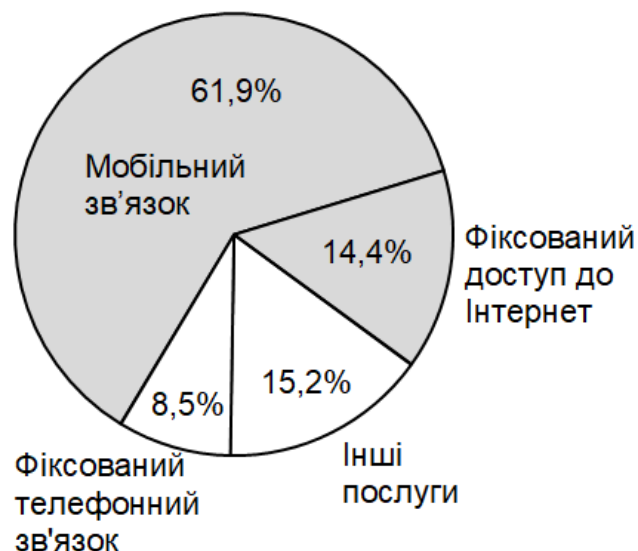


Рис. 1. Структура доходів від надання телекомунікаційних послуг за 2018 р.: фіксований телефонний зв'язок (4 786 млн. грн.); рухомий (мобільний) зв'язок (34 978 млн. грн.); фіксований доступ до мережі Інтернет (8 136 млн. грн.); інші послуги (трансляція теле- та радіо- програм та їх технічне обслуговування, супутниковий зв'язок тощо) (8 575 млн. грн.).

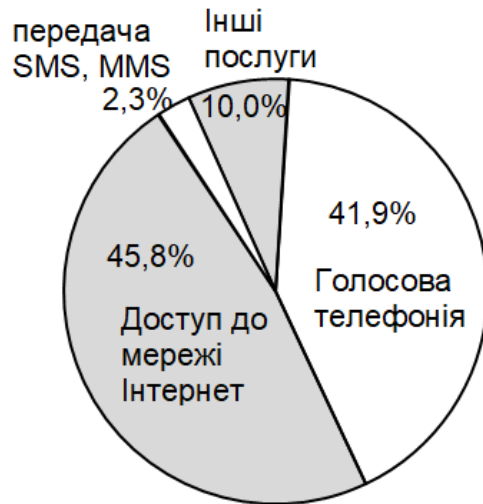


Рис. 2. Структура доходів від надання послуг рухомого (мобільного) зв'язку та їх частка у 2018 р. за даними операторів, провайдерів рухомого (мобільного) зв'язку: голосова телефонія (14 664 млн. грн.); доступ до мережі Інтернет (16 036 млн. грн.); передача SMS, MMS повідомлень, контент-послуги (807 млн. грн.); інші послуги (термінація і транзит трафіку, інші послуги, пов'язані з голосовим трафіком) (3 471 млн. грн.).

В 2018 р. доходи від надання послуг з доступу до мережі Інтернет переважили доходи від послуг голосової телефонії. Частка доходів від надання послуг з доступу до мережі Інтернет у загальному обсязі доходів рухомого (мобільного) зв'язку склала у 2018 р. 45,8%, що на 13,0% більше у порівнянні з 2017 р., при цьому частка доходів від надання послуг голосової телефонії зменшилася на 11% і склала 41,9%. Продовжується тенденція падіння обсягів передачі SMS, MMS повідомлень, частка доходів від надання таких послуг у 2018 р. склала 2,3%.

Кількість активних ідентифікаційних телекомунікаційних карток мережі рухомого (мобільного) зв'язку на кінець 2018 р. склала 54 007 тис. од.

Конфігурація пристроїв і кінцевих точок можливо з мобільних клієнтів. Після того, як вони пов'язані зі шлюзом, клієнти можуть отримати доступ до файлу конфігурації пристрою, використовуючи запит GET. Ресурс API

конфігурації надає тільки ті атрибути, які можуть бути створені або оновлені користувачами, наприклад, місце розташування.

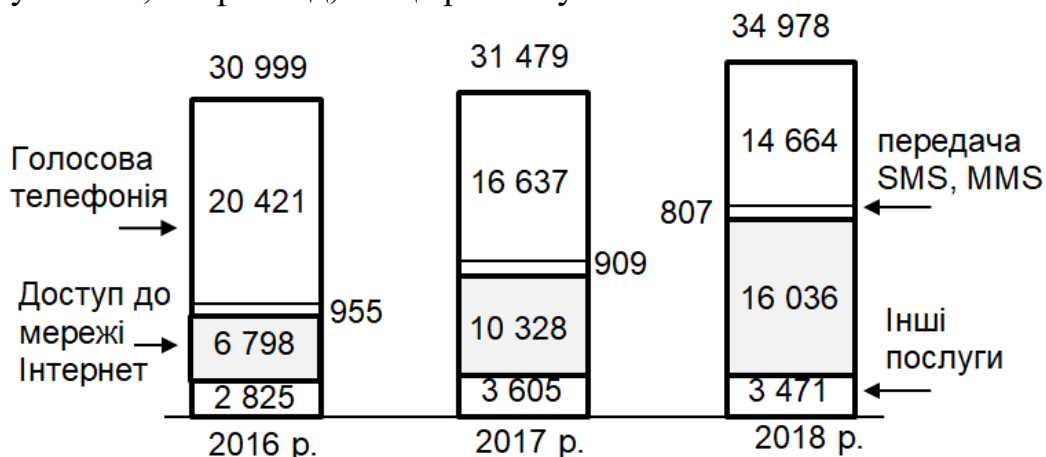


Рис. 3. Динаміка отриманих доходів від надання послуг рухомого (мобільного) зв'язку за 2016-2018 рр., млн. грн.

За прогнозами Cisco Systems (звіт Cisco VNI Global Mobile Data Traffic Forecast (2016-2021)), до 2021 р мобільний трафік даних досягне наступних показників:

- частка мобільного трафіку даних складе 20% всього IP-трафіку (в 2016 р. цей показник становив лише 8%);
- на душу населення припадатиме 1,5 мобільні пристрої, близько 12 млрд. пристроїв, підключених до мобільних мереж, включаючи модулі міжмашинного зв'язку (показники 2016 р. - 8 млрд. пристроїв і 1,1 пристрої. на душу населення);
- швидкість мобільних підключень збільшиться втричі і до 2021 р. досягне 20,4 Мбіт/с (показник 2016 р. - 6,8 Мбіт/с);
- M2M-з'єднання представлятимуть 29% (3,3 млрд.) всіх мобільних підключень (показник 2016 р. - 5% (780 млн.)). З поширенням IoT-застосувань в споживчому і бізнес-сегментах M2M стане самим швидкозростаючим типом мобільного з'єднання;
- на частку 4G до 2021 р. припадатиме 58% всіх мобільних з'єднань (в 2016 р. - 26%) і 79% всього мобільного трафіку передачі даних;
- загальне число смартфонів досягне 6,2 млрд. і перевищить половину всіх пристроїв і підключень (показник 2016 р. - 3,6 млрд.).

До 2021 р. глобальний трафік мобільної передачі даних досягне 49 ексабайт на місяць, або 587 ексабайт на рік. Еквівалент прогнозованого річного приросту (587 ексабайт на рік): це в 122 рази більше, ніж весь глобальний мобільний трафік, згенерований всього 10 років тому, в 2011 р.; це 131 трлн. зображень (наприклад, MMS).

Література

1. Ільченко М.Ю., Кравчук С.О. Телекомунікаційні системи. – К.: Наукова думка, 2017.
2. Advanced in the telecommunications 2019: monograph / by edited M.Y. Ilchenko, S.O. Kravchuk, Kyiv, 2019, 336 p. (ISBN 978-617-7734-12-2).

АЛГОРИТМ РОЗМІЩЕННЯ БАЗОВИХ СТАНЦІЙ ДЛЯ МАСШТАБНИХ ГЕТЕРОГЕННИХ МЕРЕЖ LTE

Хлівний Д.Ю., Кравчук С.О.

Інститут телекомунікаційних систем КПІ ім. І. Сікорського, Україна

E-mail: dkhlivniy@gmail.com

Base Station Placement Algorithm for Large-Scale LTE Heterogeneous Networks

In this paper represents new evolutionary algorithm for optimal base station grouping and deployment, which help us to overcome modern problems with interference in urban area and optimize their network characteristics , including throughput .

На даний час продовжується значне зростання мобільного трафіку, особливо в умовах міст, що змушує операторів розгортати ще більше нових базових станцій (безпроводових точок доступу) і підвищувати тим самим, матеріальні затрати на розгортання стандартних макростільників із зростанням інтерференції. Такий підхід є малоефективним та недоцільним в реаліях сучасного структурованого суспільства, яке постійно розвивається та потребує для свого обслуговування інформаційних каналів із підтримкою заданої якості.

Останнім часом розробки щодо оптимального розміщення базових станцій (БС) є певним випробуванням для задач оптимізації мобільної мережі. Алгоритми, що використовувалися раніше для оптимального розгортання стільників, вже застарілі та не дають можливості максимізувати пропускну здатність мережі [1, 2].

Значні проблем виникають при встановленні БС в умовах міста, де на малій площі є велике скупчення (густина) людей та високоповерхових забудов. Оптимальним рішенням в даній ситуації є доповнення вже існуючих макростільників новими мікростільниками, які будуть розміщуватися локально в місцях великого навантаження (використання трафіку), та матимуть малі вихідні потужності передачі для мінімізації проблем інтерференції в певній локації. Наступним кроком буде повне згортання макростільників та їх заміна множиною мікростільників. З даного твердження випливає інша проблема – ефективне групування БС між собою, оскільки даний підхід суттєво збільшує кількість стільників, що при їх

незапланованому розгортанню може викликати погіршення характеристик усієї мережі.

Тому для вирішення зазначених проблем оптимізації розгортання БС стає актуальною розробка нового підходу, який дозволить розширити можливості операторів щодо розгортання нових БС, мінімізувати інтерференцію і при цьому реалізувати максимально можливе значення пропускної здатності. В цьому сенсі, головною метою даної роботи є розробка методу, що призначений для вирішення вище зазначеної проблеми, шляхом використання спеціального еволюційного алгоритму, та проведення аналізу отриманих результатів моделювання сценарію безпроводової мережі із задіянням такого алгоритму

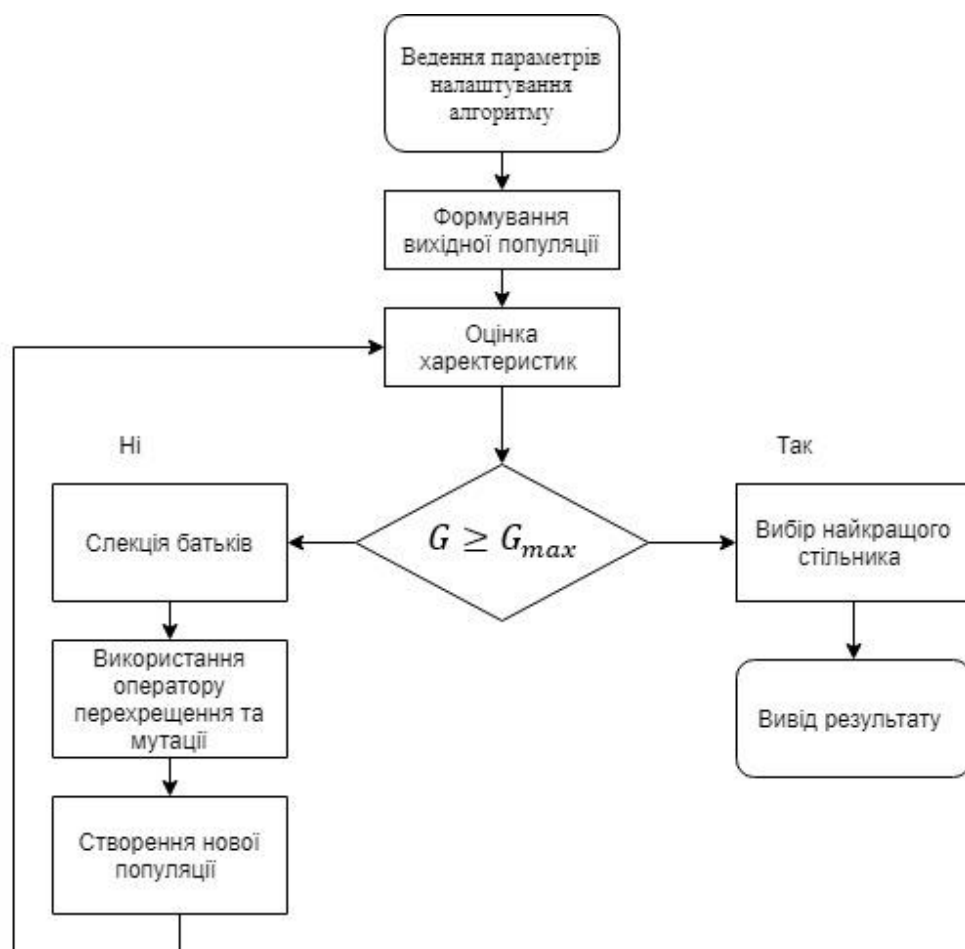


Рис. 1. G – номер теперішнього покоління; G_{max} -максимальне число поколінь, що було задане на початку роботи алгоритму [4].

Алгоритм, що запропоновано в даній роботі, є одним із можливих варіантів вирішення проблеми, що наведена вище. Сама сутність такого алгоритму полягає в групуванні БС, яке може бути поділене на наступні кроки: оцінка характеристик представлених БС; вибірка БС за знайденими

характеристиками; використання оператора схрещування; використання оператора мутації. Така послідовність дій дає можливість ефективного групування БС в популяції. Робота алгоритму представлена на схемі, що наведена на рис. 1.

В результаті маніпуляцій з БС, які наведені в схемі на рис. 1, отримуємо результат групування БС, який в свою чергу, дозволяє підвищити показники мережі, та не допустити виникнення надлишкової інтерференції.

В результаті симуляції показано, що даний алгоритм групування та розгортання БС в залежності від сценарію розташування користувачів, демонструє більші значення пропускної здатності ніж стандартні алгоритми. Також, в порівнянні з ними даний алгоритм показує результат, який в деяких випадка суттєво підвищує характеристики самої мережі. Результати, отримані в результаті симуляції, продемонстрували, що представлений алгоритм мінімізує вплив інтерференції на мережу та одночасно максимізує її пропускну здатність.

Таким чином, алгоритм, що запропоновано, дозволяє вирішити проблему високого нарощування використання трафіку в умовах міста, та в свою чергу дає можливість оптимізувати процес розгортання нових БС без значного підвищення інтерференції в мережі в цілому. Також, він є більш оптимальним із затратної точки зору, оскільки не передбачає розвертання великої кількості базових станцій, а фокусується на підтриманні якості вже наявної мережі, або на нарощуванні нових мікростільників.

Література

1. Ільченко М.Ю., Кравчук С.О. Телекомунікаційні системи. – К.: Наукова думка, 2017.
2. Lee, S., Lee, S., Kim, K., & Kim, Y. H. Base station placement algorithm for large-scale LTE heterogeneous networks. PloS one, 10(10), (2015).
3. Cortinhal M.J., Captivo M.E. Genetic algorithms for the single source capacitated location problem: a computational study // Proceedings of 4th Metaheuristics International conference, Porto, Portugal, 2001. М Р. 355М359.
4. Єрмолаєв С.Ю. Оптимальне розміщення базових станцій // TELECOMMUNICATION SCIENCES VOLUME JULY– DECEMBER 2010 с. 32.

БЕЗПРОВОДОВА КООПЕРАТИВНА РЕТРАНСЛЯЦІЯ З ТЕХНОЛОГІЄЮ HARQ

Афанасьєва Л.О., Кравчук С.О., Шевченко І.І., Чуб М.М.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: liana.afanasyeva@gmail.com

Wireless cooperative relaying with the HARQ

The paper describes a hybrid automatic request (HARQ) protocol for cooperative relaying, considering the advantage of using cooperative schemes. The proposed algorithm for selecting the relay method allows to increase the capacity and energy efficiency of the system.

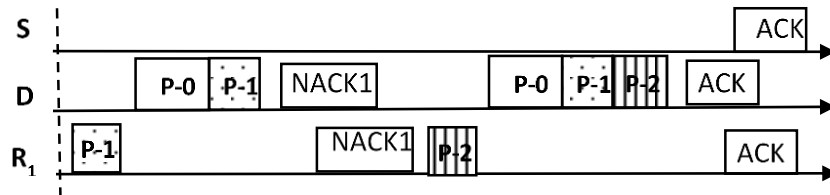
Оскільки кінцевою метою будь-якої комунікаційної системи є підвищення загальної продуктивності, стає необхідним розробити схему роботи протоколу HARQ при кооперативній передачі даних, що дозволяє збільшити пропускну здатність і енергоефективність системи [1-3].

Основна ідея кооперативного HARQ протоколу полягає в тому, щоб об'єднати кооперативний (cooperative) ARQ (C-ARQ) протокол з HARQ, щоб використовувати переваги обох схем. Схема передачі даних C-ARQ реалізовує просторове рознесення, а HARQ надає можливості виправлення помилок, що дозволяє досягти високої пропускну здатності та продуктивності безпроводової мережі [4]-[5].

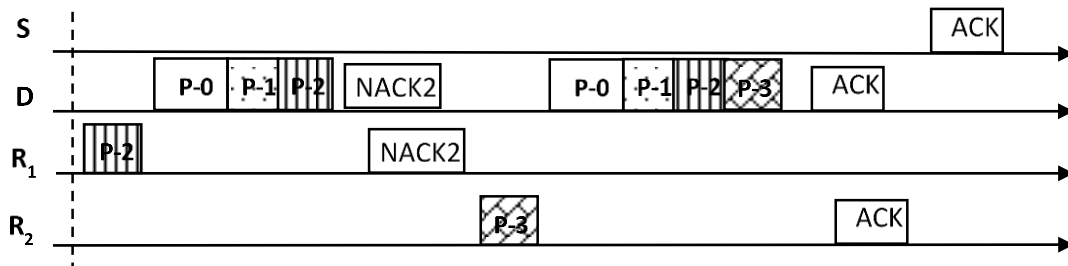
Джерело S (source) починає фазу 1, передаючи пакет $P-0$ до цільового приймача D (destination). Ця передача, яка є широкомовною за своєю природою, також «підслуховується» допоміжними терміналами-ретрансляторами R . На цільовому приймачі D до отриманого пакету $P-0$ застосовується метод виявлення помилок. Кожен вузол R обчислює циклічний надлишковий код CRC (cyclic redundancy code) для перевірки помилок в підслуханому пакеті $P-0$. Ті термінали-ретранслятори R , які отримали пакет $P-0$ без помилок, кодують його в $P-1, P-2 \dots P-N$ відповідно та зберігають у верхній частині свого буфера пакетів.

Якщо в отриманому на цільовому приймачі пакеті $P-0$ немає помилок, то відправляється ACK до джерела S . Після перехоплення ACK, вузли R скидають поточні пакети з FEC кодами з верхньої частини свого буфера. Якщо ж в отриманому пакеті $P-0$ виявлена помилка, то цільовий приймач D зберігає пакет з помилкою $P-0$ в буфері та переходить у фазу 2 (кооперативної ретрансляції), передаючи сигнал «Запит на кооперацію» (CoopReq). Джерело S продовжує залишатися в режимі «очікування», чекаючи відповідь сигналу ACK або NACK. Доступні вузли R відповідають на CoopReq, передаючи сигнали «Готовий для кооперації» (CoopReady) на цільовий приймач D . Після передачі CoopReq D очікує час T_c , щоб всі доступні сигнали досягли D до початку фази кооперативної ретрансляції. Після закінчення часу очікування T_c D зберігає всі отримані сигнали CoopReady у вигляді списку. Цей список використовується для вибору або

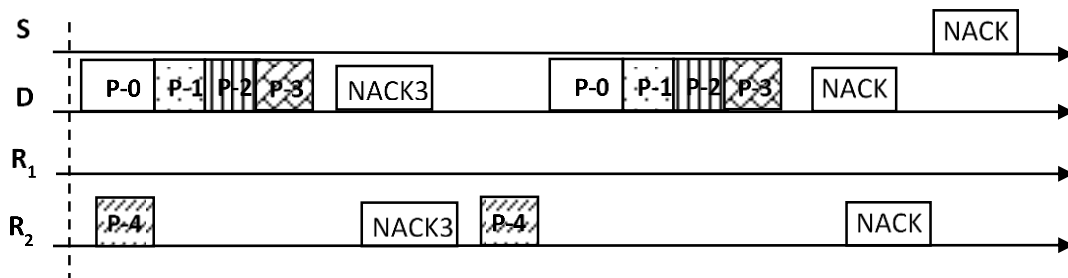
пошуку допоміжних терміналів-ретрансляторів R у фазі кооперативної ретрансляції. Сигнал *CoopReq* може містити кілька полів для зберігання інформації, пов'язаної з доступними вузлами R , такі як відстань R - D , що рівень енергії, рівень с/ш, що дозволить D застосувати критерій вибору для сортування списку в певному порядку.



а) кооперативна ретрансляція з одним допоміжним терміналом-ретранслятором;



б) кооперативна ретрансляція з двома допоміжними терміналами-ретрансляторами;



в) неуспішна кооперативна ретрансляція;

Рис.1. Алгоритми безпроводової кооперативної ретрансляції з технологією HARQ.

Процес встановлення зв'язку з вузлом R включає в себе передачу *NACK-j* на заданий вузол R - i із запитом пакету з FEC кодами P - j . Наприклад, цільовий приймач відправляє *NACK-1* в вузол R -1, термінал-ретранслятор R -1 передає пакет P -1 на D , де він зберігається та перевіряється на наявність помилок, обчислюючи CRC. Після чого, цільовий приймач D відновлює вихідні дані, комбінуючи збережені пакети P -0 і P -1.

Для відстеження наявності помилок в збережених пакетах з FEC кодами на цільовому приймачі застосовується спеціальна мітка стану *state_tag*, де *state_tag* = 1 означає, що прийнятий пакет з FEC кодами не містить помилок і не вимагає повторної передачі, а *state_tag* = 0 означає, що збережений пакет має деякі помилки і, отже, може знадобитися повторна передача.

Якщо відновлення пройшло успішно, ACK надсилається джерелу і фаза кооперативної ретрансляції закінчується. В іншому випадку, відправляється *NACK-2* на R -1 для наступного пакета з FEC кодами, P -2. Отримавши P -2, D

зберігає його з відповідною міткою стану, а потім використовує в наступній спробі декодування разом з попередньо збереженими пакетами.

Розглянемо випадок, коли після двох передач ($M = 2$) вихідний пакет не декодовано без помилок. Це відбувається через наступні можливі причини: тільки одного безпомилкового пакета з FEC кодами недостатньо для виправлення помилок в збереженому $P-0$ або всі збережені пакети з FEC кодами безпомилкові, але збережений вихідний пакет $P-0$ має велику кількість помилок.

У першому випадку D вибирає наступний в списку термінал-ретрансляції $R-2$ для фази кооперативної передачі. Цільової приймач перевіряє мітки стану пакетів, щоб ідентифікувати всі неправильні пакети з FEC кодами й встановлює відповідне значення $NACK$ для передачі. Наприклад, якщо потрібна повторна передача $P-j$, значення $NACK$ встановлюється j . Таким чином, якщо $R-2$ отримує $NACK-j$, то знаходить пакет $P-j$ в своєму буфері та ретранслює до D . Цільовий приймач перезаписує збережений $P-j$, виконує виявлення помилок і відповідно оновлює мітку стану. Декодування вихідного пакета $P-0$ виконується з використанням всіх пакетів, збережених в буфері, включаючи новий. При успішному відновленні даних, відправляється ACK до джерела та припиняється фаза кооперативної ретрансляції.

У другому випадку, коли всі пакети з FEC кодами були правильно прийняті (тобто $state\_tag = 1$ для всіх пакетів з FEC кодами), відправляється $NACK$ до джерела S . Після отримання $NACK$ джерело S виходить з режиму очікування та передає нову копію $P-0$, яка використовується цільовим приймачем D в наступній спробі виправлення помилок.

У роботі описано системну модель для реалізації протоколу HARQ для безпроводових систем, що враховує перевагу використання кооперативних схем. Збільшення пропускної здатності системи та енергоефективності кооперативної передачі досягається за рахунок передачі допоміжними терміналами-ретрансляторами лише даних для виправлення помилок.

Література

1. S. Kravchuk, L.Afanasyeva Wireless cooperative relaying without maintaining a direct connection between the source and target receiver terminals// Information and Telecommunication Sciences, No 2, pp. 5-11, 2019 (DOI: <https://doi.org/10.20535/2411-2976.22019.5-11>).
2. Афанасьєва Л.О., Кравчук С.О. Протокол адаптивної ретрансляції для кооперативних мереж// Матер. 13-ї міжнар. наук.-техн. конф. “Перспективи телекомунікацій”, 15-19 квітня 2019 р. – К.: КПІ ім. Ігоря Сікорського, 2019. – С. 192–195.
3. Льченко М.Ю., Кравчук С.О. Телекомунікаційні системи. – К.: Наукова думка, 2017.
4. Maaz M., Lorandel J., Mary Ph. Energy efficiency analysis of hybrid-ARQ relay-assisted schemes in LTE-based systems// EURASIP Journal on Wireless Communications and Networking. – №22, 2016 (<https://doi.org/10.1186/s13638-016-0520-9>).
5. Maliqi F., Bassi F., Duhamel P., Limani I. Simplified analysis of HARQ cooperative networks using finite-state Markov chains // 25th European Signal Processing Conference (EUSIPCO), 28 Aug.-2 Sept. 2017. –p.2006-2010 (doi:10.23919/eusipco.2017.8081561).

УЗАГАЛЬНЕНА СТРУКТУРА СИСТЕМИ МОБІЛЬНИХ ІНФОКОМУНІКАЦІЙ

Рисцова К.І., Остапов О.А., Кравчук С.О.

Інститут телекомунікаційних систем КПІ ім. І. Сікорського, Україна

E-mail:sakravchuk@ukr.net

The generalized structure of the mobile infocommunication system

A simplified generalized structure of a mobile infocommunication system is presented, which has the ability to connect various types of radio access networks to the core network, as well as the presence of intelligent nodes (functions) of the signaling network that support mobility, autonomy, and self-organization of the entire mobile infocommunication network.

Інфокомунікаційна безпроводова мобільна система користувацького доступу – стільникова система мобільного зв'язку (ССМЗ) є повноцінною інформаційно-телекомунікаційною системою, а до її функцій відносяться базові функції телекомунікаційної системи: передавання (перенесення) інформації; сигналізація (внутрішнє керування системи); комутація інформаційних потоків (пакетів); загальне керування.

Узагальнена структура одно-стільникової системи мобільного зв'язку для одного користувача представлено на рис. 1, а для повно-стільникової системи мобільного зв'язку – на рис. 2.

Найбільш простим випадком є одно-стільникова система мобільного зв'язку для обслуговування одного користувача – одного мобільного терміналу (МТ) (рис. 1). В даному випадку маємо систему взаємодії трьох основних об'єктів: МТ, безпроводова мережа доступу (мережа радіодоступу) і базова транспортна мережа надання послуг. МТ забезпечує через радіоінтерфейс з'єднання із точкою доступу (базовою станцією) мережі радіодоступу. Через точку доступу виконується обмін інформацією між МТ і центром комутації та маршрутизації базової транспортної мережі надання послуг. Центр комутації є ключовим вузлом базової мережі і формує усі з'єднання для МТ, виконуючи при цьому його аутентифікацію і тарифікацію за допомогою спеціальної бази даних користувача оператора мережі. Мається на увазі, що даний МТ вже зареєстрований в даній базовій мережі. Також центр комутації виконує з'єднання з іншими центрами мережі оператора та зовнішніми мережами. Загальне керування за мережею оператора виконує Центр керування.

При цьому можна зазначити наступні стадії роботи МТ в мережі оператора:

- входження в зв'язок;
- аутентифікація;
- реалізація підключень каналу трафіку в мережі.

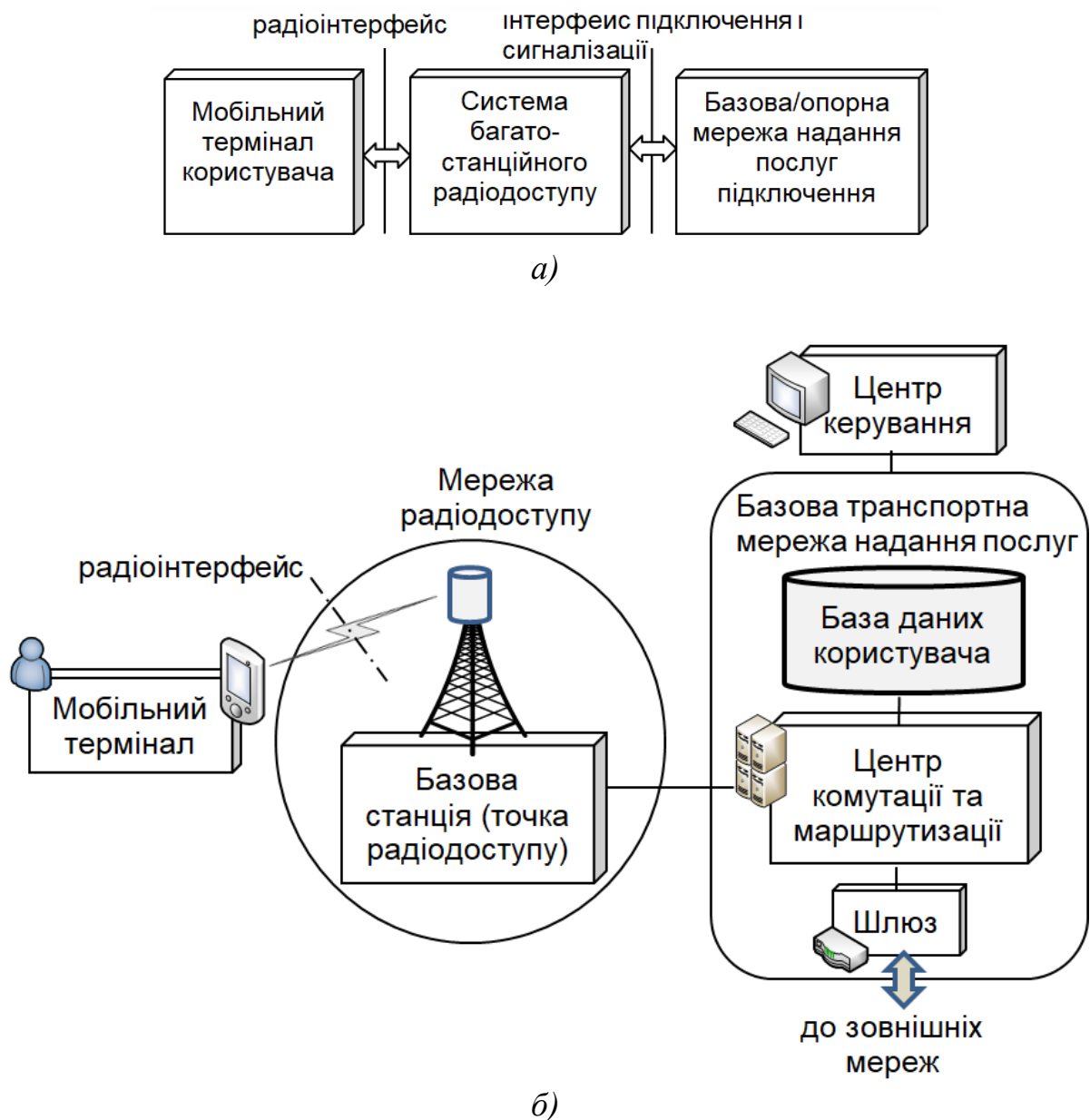


Рис. 1. Базові складові (а) та узагальнена структура (б) одно-стілнкової системи мобільного зв'язку для одного користувача.

При наближенні до реальності, як у більш складному випадку, має місце велике і різноманітне розгалуження мережі оператора ССМЗ з відповідно більш складною архітектурою (рис. 2). Наприклад, розглянемо випадок, коли є ряд МТ, що працюють з точками доступу в різних мережах радіодоступу. Останні мають відповідні підключення до центрів комутації неоднакових базових мереж. Причому із-за свого руху в зоні розгортання мереж радіодоступу МТ весь час змінює точки доступу, що його обслуговують. Отже для МТ повинні завжди бути хоча б три наступні види мереж: домашня, де МТ був зареєстрований і де зберігаються дані про нього; транзитна, через яку інформація, призначена для МТ, проходить транзитно, тобто без обробки (її наявність необхідна тільки у тому випадку, коли мережа, що обслуговує, не має безпосереднього з'єднання із домашньою

мережею MT); обслуговуюча – це мережа яка на даний момент часу обслуговує MT (вона не може бути транзитною). Усі зазначені мережі можуть бути зовсім різними за своєю структурою і вмістом.

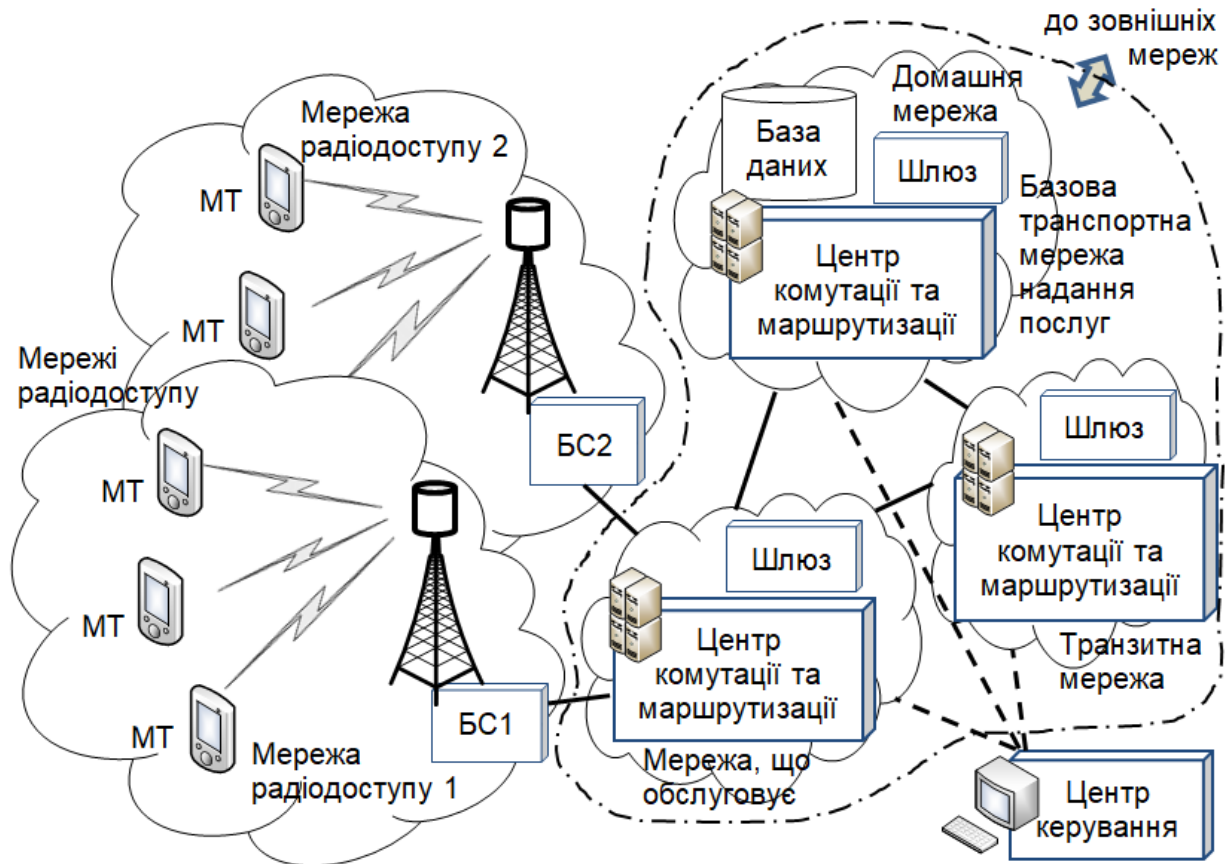


Рис. 2. Узагальнена мережна структура стільникової системи мобільного зв'язку одного оператора.

Для того, щоб мережу, що зображено на рис. 2, можна було віднести до сучасної повноцінної системи мобільних інфокомунікацій необхідне врахування можливості підключення до опорної мережі різних типів мереж радіодоступу, а також наявність інтелектуальних вузлів (функцій) мережі сигналізації, що забезпечують підтримку мобільності, автономісті та самоорганізації всієї мережі мобільних інфокомунікацій. Так на рис. 3 представлено спрощену узагальнену структуру системи мобільних інфокомунікацій. Доступ MT користувача до опорної мережі може бути як безпроводовим, так і проводовим. Причому радіодоступ може бути реалізований в межах стільників з різними технологіями безпроводового доступу, наприклад, багатостанційний доступ з часовим розділом TDMA (time division multiple access), багатостанційний доступ з кодовим розділом CDMA (Code Division Multiple Access) і багатостанційний доступ з ортогональним частотним розділенням каналів OFDMA (Orthogonal frequency-division multiple access). Для забезпечення необхідних інтерфейсів з БС, що працюють в різних безпроводових стандартах, використовується інтерфейсний контролер, який також може забезпечити інтерфейс взаємодії

між цими БС і проводовими каналами доступу. Основу сигналізації опорної мережі складають вузол керування мобільністю, що забезпечує підтримку неперервної передачі обслуговування і сервіс визначення місцеположення користувацького терміналу та БС, база даних користувачів (ідентифікатори, параметри обслуговування та ін.) та функція правил і політики обробки викликів і тарифікації, що забезпечує інтелектуальну політику функціонування мережі та обслуговування кожного користувача у відповідності до встановлених вимог якості обслуговування затребуваних сервісів.

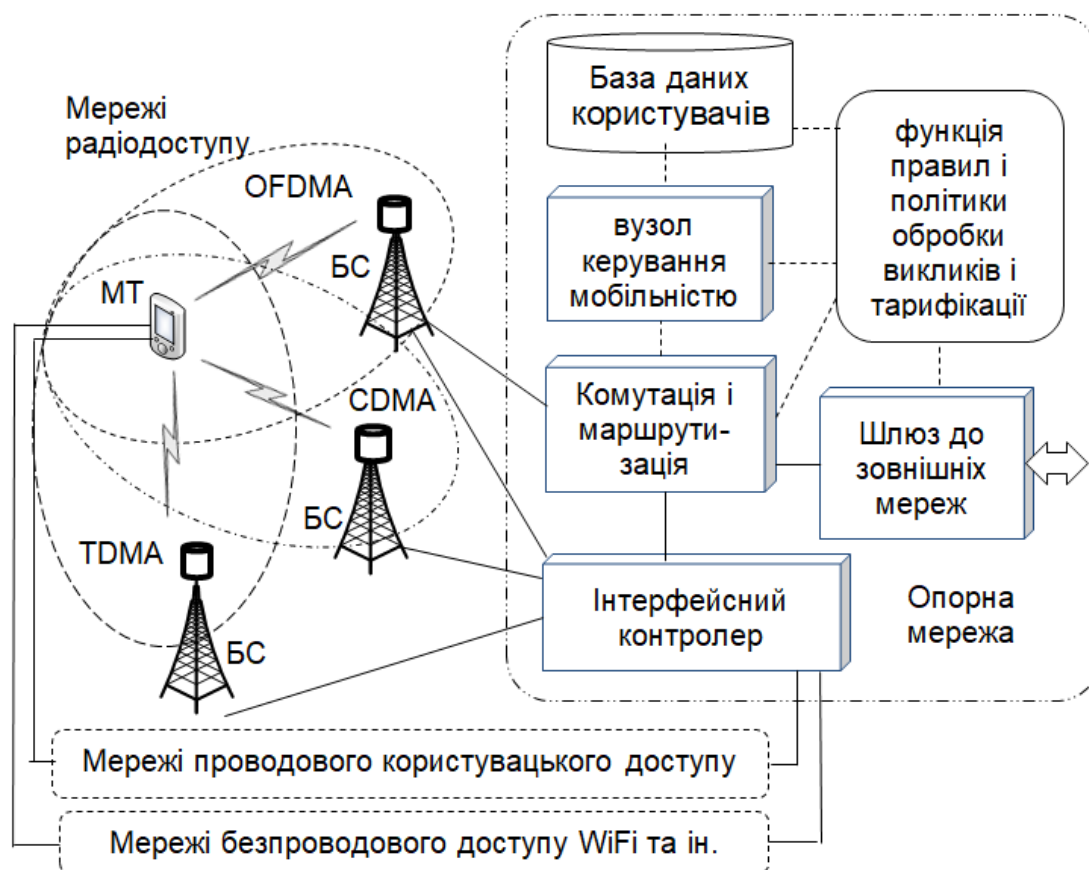


Рис. 3. Спрощена узагальнена структура системи мобільних інфокомунікацій.

В даному випадку МТ користувача може функціонально бути звичайним мобільним телефоном/смартфоном, допоміжним пристроєм для підключення до проводових мереж доступу, контрольованих оператором, та терміналом послуг міжмашинної взаємодії M2M і Інтернету речей IoT.

Література

1. Ільченко М.Ю., Кравчук С.О. Телекомунікаційні системи. – К.: Наукова думка, 2017.
2. Advanced in the telecommunications 2019: monograph / by edited M.Y. Ilchenko, S.O. Kravchuk, Kyiv, 2019, 336 p. (ISBN 978-617-7734-12-2).

ЕКСПЕРИМЕНТАЛЬНЕ ВІДПРАЦЮВАННЯ РЕТРАНСЛЯЦІЙНИХ ВУЗЛІВ СУЗІР'Я ДРОНІВ

Кравчук С.О., Кайдено М.М., Афанасьєва Л.О., Кравчук І.М.

Інститут телекомунікаційних систем КПІ ім. І. Сікорського, Україна

E-mail:sakravchuk@ukr.net

Experimental testing of the relay node drones constellation

The main goal of this work is the experimental development of the basic principles of controlling a swarm (constellation) of drones and the formation of a cooperative relay system, which were theoretically justified and defined in earlier works of the authors.

Основною метою даної роботи є експериментальне відпрацювання базових принципів керування рою (сузір'я) дронів та формування кооперативної системи ретрансляції, що були теоретично обґрунтовані та визначені в ранішніх роботах [1-5].

Рій (сузір'я) дронів був сформований із 5 квадрокоптерів Syma X8 PRO, причому тільки три з них (позиції 2, 3, 4 на рис. 1) були оснащені додатковими трансиверами на базі ADALM-Pluto Radio (рис. 2) і без відеокамери, ще два дрона (позиції 1 і 5 на рис. 1) виконували функцію постановників додаткових завдань в каналах керування.

Наземна система керування (НСК) складалась із: пультів керування дронів Syma, об'єднаних через Bluetooth-канали з комп'ютером керування (КК) так, що з КК можна було керувати їх польотом (кожного окремо); приймально-передавального блоку на базі ADALM-Pluto Radio, який підключений до того ж КК, основною функцією якого було забезпечення радіоканалів обміну даних з дронами та кооперація між ними.



Рис. 1. Зависання рою дронів на висоті 35...40 м (жовтень 2019 р.)

Квадрокоптер Syma X8 PRO є досить великим літальним апаратом (50x50x19 см), політ якого цілком стабільний в безвітряну погоду і при

слабкому вітрі. Бовтанка виникає при швидкості вітру в 4-5 м/с і вище. Час польоту в значній мірі залежить від погодних умов, але не перевищує 8-9 хвилин. Дальність керування досягає 200 м. Квадрокоптер укомплектований класичними колекторними двигунами, що забезпечують плавний і рівний політ. Додаткова вантажопідйомність Syma X8 Pro становить 200 г.

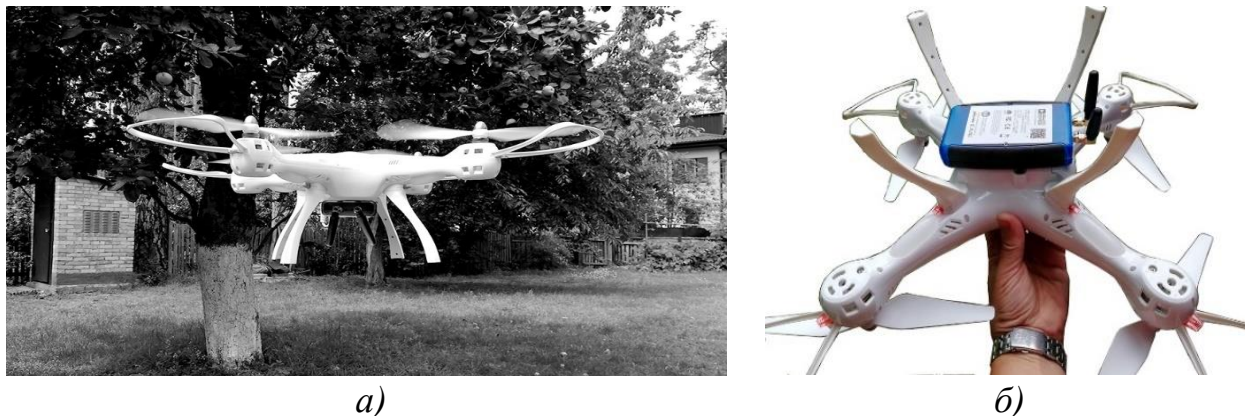


Рис. 2. Зображення квадрокоптера Syma X8 PRO із модулем ADALM-Pluto Radio.

Інтегрований датчик тиску дозволяє машині зберігати висоту, а в поєднанні з блоком GPS і 6-осевим гіроскопом - ще й утримувати позицію (функція Hover). Система безпеки польотів представлена кількома різновидами режиму автоматичного повернення (RTH) і «безголовим» режимом. Квадрокоптер Syma X8 PRO оснащений FPV (Wi-Fi) HD-камерою, яка дозволяє як записувати фото і відео на карту пам'яті, так і передавати на телефон в режимі реального часу. В ході польотів від першої особи дрон здатний летіти на 70 м. Каналом відеозв'язку є звичайний Wi-Fi, який працює в діапазоні 2,4 ГГц. Застосування для підключення квадрокоптера до смартфона можна скачати на Play Market або App Store.

Портативний автономний модуль (Design software-defined radio, SDR) радіочастотного навчання Analog Devices ADALM-Pluto Radio заснований на високо інтегрованому високочастотному приймально-передавальному чіпі AD9363 компанії Analog Devices і FPGA Zynq Z-7010 компанії Xilinx (рис. 3). Перекриває частоти в діапазоні від 325 МГц до 3,8 ГГц, миттєва ширина смуги до 20 МГц, змінна швидкість обміну даними, 12-розрядні АЦП і ЦАП, містить один передавач і один приймач, може працювати як в повнодуплексному, так і в напівдуплексному режимі, підтримка MATLAB і Simulink, блоки приймача і передавача GNU Radio.

Для керування модулем було використано програмне забезпечення бібліотеки «Communications Toolbox Support Package for Analog Devices ADALM-Pluto Radio» (<https://se.mathworks.com/help/supportpkg/plutoradio/index.html>).

Послідовність роботи експериментальної системи наступна. Спершу кожен з дронів окремо був піднятий на висоту зависання за допомогою системи керування Syma. Запуск усіх дронів одразу, нажалі, із-за пересічних завад

системи керування не вдалося.

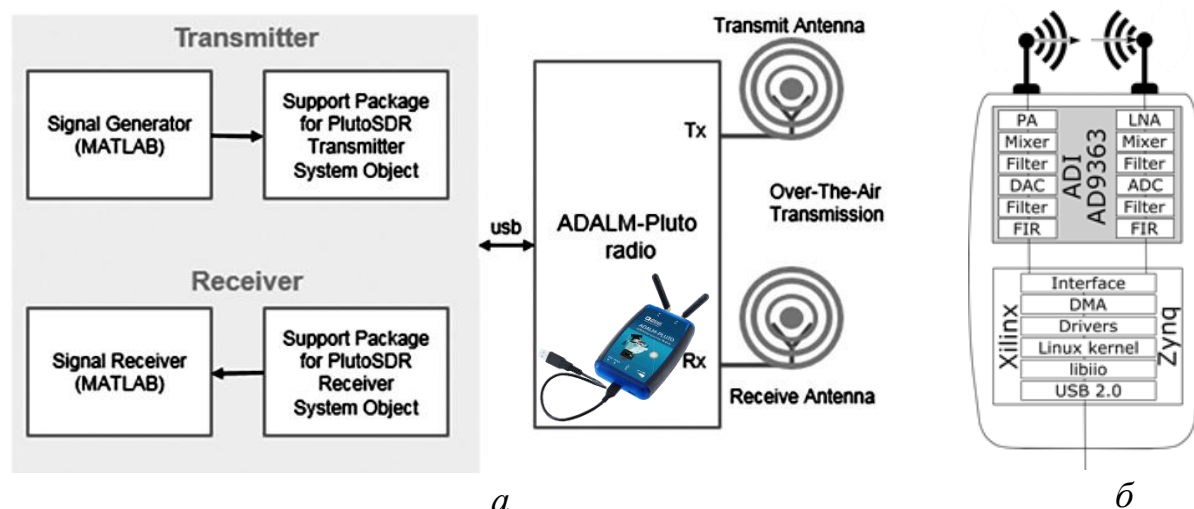


Рис. 3. Структурні схеми:

- а) взаємодії між Simulink, блоком передавача Pluto і радіоустаткуванням;
б) модуля ADALM PLUTO.

Три експериментальні дрони послідовно підключались (подавався потік даних) так, щоб сигнал на приймачі НСК був мінімальний, але при якому ще можливе підтримання радіозв'язку QPSK із допустимим рівнем бітових помилок (орієнтовно 10^{-4}). При цьому заміри відношення сигнал/шум від дронів склали 11-12 дБ. Потрібно відмітити, що головним мінусом модулів ADALM-Pluto є їх нестабільність частотної опори. Тому весь час (на початку передачі наступного барсту) проводилась синхронізація модулів. В режимі традиційної кооперативної ретрансляції цільовим приймачем був дрон 2 або 4, дрон 3 виконував функцію кооперативного ретранслятора. Джерелом сигналу і системою керування кооперативної роботи дронів виступав КК і наземний модуль ADALM-Pluto. Перехід системи в режим кооперативної ретрансляції дозволив підвищити енергетику радіолінії до дронів на 2-3 дБ.

Література

1. Advanced in the telecommunications 2019: monograph / by edited M.Y. Ilchenko, S.O. Kravchuk, Kyiv, 2019, 336 p. (ISBN 978-617-7734-12-2).
2. Kravchuk S., Afanasieva L. Formation of a wireless communication system based on a swarm of unmanned aerial vehicles // Information and Telecommunication Sciences. - 2019. - No 1. - 11-18 p. DOI: <https://doi.org/10.20535/2411-2976.12019.11-18>
3. Кравчук С.О. Безпілотний літальний апарат в якості мобільного M2M-шлюзу для безпроводових всепроникаючих мереж // Матер. 13-ї міжнар. наук.-техн. конф. "Перспективи телекомунікацій", 15–19 квітня, 2019 р. – К.: Хімджест, 2019. – С. 179–181.
4. Кравчук С.О., Кравчук І.М. Підходи та стратегії щодо колективного керування роєм дронів // Матер. 13-ї міжнар. наук.-техн. конф. "Перспективи телекомунікацій", 15–19 квітня, 2019 р. – К.: Хімджест, 2019. – С. 170–174.
5. Ільченко М.Ю., Кайдено М.М., Кравчук С.О. Структурно-функціональні принципи побудови системи управління та зв'язку бортового і наземної обладнання телекомунікаційної мережі на основі аероплатформ // Матер. 12-ї міжнар. наук.-техн. конф. "Проблеми телекомунікацій", 16–20 квітня, 2018 р. – К.: Хімджест, 2018. – С. 26–29.

МЕТОДИ ЗАБЕЗПЕЧЕННЯ ЗАДАНИХ ПОКАЗНИКІВ БЕЗПЕКИ В 5G МЕРЕЖАХ

Правило В.В., Кормульов О.С.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: v.v.pravylo@ukr.net, steallex214@gmail.com

Methods of ensuring specified security indicators in 5G networks

In this paper, we consider several possible threats in 5G networks and also discover a methods for solving them.

З швидким розвитком мобільних мереж п'ятого покоління постає питання в забезпеченні безпеки в цих мережах. Незважаючи на те, що в стандарти 5G включені вбудовані функції безпеки, самої по собі мережевої інфраструктури недостатньо для вирішення всіх проблем, пов'язаних з безпекою. На відміну від мереж попередніх поколінь, 5G підтримує більше видів послуг та має більш широкий спектр задач. Такі технології, як пристрої, підключені до Інтернету речей (IoT), доповненої реальності (AR), віртуальної реальності (VR) та інші, вимагають швидкої, надійної та обширної мережі, щоб не відставати від темпів розвитку. Нові підприємства та нові технології, що працюють в епоху 5G, зіткнуться з новими проблемами безпеки та конфіденційності.

Майбутні мережі зв'язку 5G не тільки успадкують уразливості мереж четвертого покоління, а й можуть обзавестися новими недоліками безпеки. Поряд з високою швидкістю (в 10-1000 разів більшою ніж у 4G), низьким енергоспоживанням і мінімальними затримками сигналу, очікується активне використання в мережах 5G технологій віртуалізації мережевих функцій (Network Function Virtualization). Заміна апаратних елементів програмними має багато позитивних ефектів, проте потенційно зробить стільникові мережі ще більш уразливими для атак зловмисників.

Проведемо аналіз вразливих місць в 5G за допомогою простого прикладу – модельна неопублічна 5G-мережа (Non-Public Network, NPN) підключену до зовнішнього світу через канали зв'язку загального користування (Рис. 1).

Саме такі мережі будуть використовуватися в найближчому майбутньому. Потенційне середовище розгортання мереж такої конфігурації - «розумні» підприємства, «розумні» міста, офіси великих компаній і інші аналогічні локації з високим ступенем контролюваності.

Як показано на Рис 1., NPN має фундаментальну вразливість у своїй конструкції. Система безпеки, яка працює у внутрішніх мережах NPN, захищає об'єкт і його приватне хмарне сховище, система безпеки вбудована в систему - свою внутрішню інфраструктуру. Трафік між NPN і зовнішніми мережами вважається безпечним, оскільки виходить з захищених систем, але фактично його нічого не захищає. На цій ділянці відсутній видимий ІТ-

моніторинг безпеки. Багато роумінгових-, міжміських-, радіо- та інших видів атак, можуть спричинити компрометацію інформації, а отже, і самої мережі 5G.



Рис. 1. Непублічна 5G мережа. Закрита мережа підприємства підключена до глобальної 5G-мережі через публічні канали.

Виникає декілька можливих сценаріїв кібератак на мережі 5G, які експлуатують:

- Уразливості SIM-карт
- Уразливості мережі
- Уразливості систем ідентифікації

При атаках апаратного рівня може використовуватися метод віддалених маніпуляцій з SIM-картою (SIMjacking) в роумінгу (тобто при роботі поза "домашньої" мережі). Наприклад, модифікація її налаштувань таким чином, щоб пристрій користувача підключався не до публічної мережі, а до мережі, якою керують кіберзлочинці. Завдяки змінам в налаштуваннях SIM-карти хакери зможуть здійснювати прослуховування розмов користувача, впроваджувати шкідливі програми та заважати алгоритмам машинного навчання.

При атаках на дані і саму мережу, зламана SIM-карта використовується для того, щоб погіршити продуктивність самого пристрою і мережі, до якої він підключений або навіть змінити базові налаштування цієї мережі. Атаки salami і low-and-slow дозволять з часом створити в інфраструктурі мережі "сліпі плями", які хакери зможуть використовувати для більш масштабних кібератак.

В атаках із застосуванням телекомунікаційних каналів і посвідчень повноважень доступу, зловмисники користуються тим, що існує певна невідповідність між способами обробки посвідчень ідентифікації в ІТ-системах і цих каналах. Велика частина посвідчень і облікових даних в телекомунікаційних каналах прив'язана до SIM-картки і обробляється на

апаратному рівні, а в IT-інфраструктурі - на рівні ПО. Відповідно, після крадіжки особистості користувача за допомогою злому карти, хакери отримують доступ і до IT-систем, які налаштовані так, щоб автоматично "довіряти" пристрою з цієї SIM-картою. В результаті цього, вони можуть використовувати цю вразливість для обходу систем захисту від шахрайських дій, змін функцій мережі і навіть змін кінцевих продуктів, якщо мова йде про виробництво.

Уразливості NPN-мережі 5G - наслідок розрізненості процедур безпеки на комунікаційному рівні, рівні SIM-карт і пристроїв, а також на рівні роумінгової взаємодії мереж. Щоб вирішити цю проблему, необхідно відповідно до принципу нульової довіри (Zero-Trust Architecture, ZTA) забезпечити перевірку справжності пристроїв, які підключаються до мережі, на кожному етапі, запровадивши федеративну модель ідентифікації та управління доступом (Federated Identity and Access Management, FIdAM).

Принцип ZTA полягає в підтримці безпеки навіть коли пристрій не підконтрольно, коли він рухається або перебуває за межами периметра мережі. Федеративна модель ідентифікації - це підхід до безпеки 5G, який забезпечує єдину узгоджену архітектуру для перевірки автентичності, прав доступу, цілісності даних і інших компонентів і технологій в мережах 5G.

Такий підхід виключає можливість впровадити в мережу «роумінгову» вишку і перенаправити на неї захоплені SIM-карти. IT-системи зможуть повноцінно виявити підключення сторонніх пристроїв і блокувати паразитний трафік, що створює статистичний шум.

Для захисту SIM-карти від модифікації необхідно впровадити в неї додаткові засоби перевірки цілісності, наприклад, реалізовані у вигляді SIM-додатку на базі блокчейна. Додаток може використовуватися для аутентифікації пристроїв і користувачів, а також для перевірки цілісності прошивки і налаштувань SIM-карти як в роумінгу, так і при роботі в домашній мережі.

Отже, рішення виявлених проблем безпеки 5G можна представити у вигляді об'єднання трьох підходів:

- впровадження федеративної моделі ідентифікації та управління доступом, яка забезпечить цілісність даних в мережі;
- забезпечення повної видимості загроз шляхом реалізації розподіленого реєстру для перевірки легітимності і цілісності SIM-карт;
- формування розподіленої системи безпеки, що вирішує питання взаємодії з пристроями в роумінгу.

Література

1. <https://www.ec-rs.ru/blog/novosti/positive-technologies-zapuskaet-servis-po-otsenke-zashchishchennosti-setey-4g-i-5g/>
2. <https://habr.com/ru/company/trendmicro/blog/486262/>
3. Craig Gibson - Securing 5G Through Cyber-Telecom Identity Federation.
https://documents.trendmicro.com/assets/white_papers/wp-securing-5g-through-cyber-telecom-identity-federation.pdf.
4. <http://www.dailycomm.ru/m/49398/>

НАДШИРОКОСМУГОВИЙ МОБІЛЬНИЙ ЗВ'ЯЗОК ЯК ОДИН ІЗ ПЕРШИХ СЕРВІСІВ 5G

Федоров С.О., Правило В.В.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: alternative1398@gmail.com, v.v.pravylo@ukr.net

Enhanced Mobile Broadband (eMBB) as one of the first 5G services

The article presents information about Enhanced Mobile Broadband (eMBB). The principles of working and implementing have been analyzed.

До недавнього часу в світі існувало чотири покоління мобільного зв'язку. Стандарт мобільного зв'язку п'ятого покоління (5G) - це новий етап розвитку технологій, який покликаний розширити можливості доступу в Інтернет через мережі радіодоступу. Серед послуг, які пропонує 5G це реалізація надширокосмугового мобільного зв'язку (Extreme Mobile Broadband, eMBB).

Надширокосмуговий мобільний зв'язок (eMBB) - це одна із трьох головних послуг, визначених для 5G. eMBB спочатку було розширенням до існуючих 4G-сервісів і одним із перших 5G-сервісів, котрі можна придбати. Стандартизацію мереж мобільного зв'язку 2, 3, 4 і 5 поколінь виконує партнерський проект для стандартизації систем 3-го покоління (3rd Generation Partnership Project, 3GPP). Щоб дозволити раннє впровадження послуг eMBB, у березні 2017 року група RAN 3GPP взяла на себе зобов'язання доопрацювати несамостійний варіант (NSA) 5G NR до березня 2018 року. Насправді стандарт був затверджений у грудні 2017 року. У режимі NSA використовується існуюча мережа 4G, доповнена 5G-носіями NR, щоб підвищити швидкість передачі даних та зменшити затримку. Таким чином, eMBB можна розглядати як першу фазу 5G, яка охоплена оновленням стандартів 3GPP Release 15. Друга фаза 5G виходить за рамки сервісів eMBB для більш трансформаційних додатків URLLC та mMTC та включена до випуску 16.

Взявши за приклад підключені автомобілі, перша фаза послуг eMBB передбачає покращені інформаційні розваги на транспортних засобах, такі як сповіщення про дорожній рух у режимі реального часу, швидкісний доступ до Інтернету, потокове відео в режимі реального часу або ігри в 3D-відео 4K. Друга фаза - це автономні транспортні засоби масового масштабу, здатні підключатися до інших транспортних засобів та навколишньої дорожньої інфраструктури та взаємодіяти з ними.

При використанні eMBB є три різних ознаки, які 5G потрібно буде досягнути:

- Більш висока пропускна спроможність - широкосмуговий доступ повинен бути у густонаселених районах, як у приміщенні, так і на вулиці, як у центрах міста, офісних будівлях або громадських місцях, таких як стадіони або конференц-центри;
- Розширений зв'язок – широкосмуговий доступ повинен бути доступний скрізь, щоб забезпечити постійний користувацький доступ;
- Більш висока мобільність користувачів – надає можливість мобільних широкосмугових послуг у русі транспортних засобів, включаючи автомобілі, автобуси, поїзди та літаки.

Ці категорії випадків використання матимуть різні вимоги. У сценарії «гарячої точки», коли на спортивному заході багато користувачів, наприклад глядачів, буде потреба у дуже високій пропускній спроможності для задоволення потреб усіх користувачів, але ці користувачі будуть статичні або рухатись повільно тому вимога до мобільності буде низькою. Навпаки, для надання послуг eMBB пасажиром у швидкісному поїзді буде потрібний високий ступінь мобільності, але ємність трафіку буде нижчою, ніж у гарячої точки.

Для забезпечення цих вимог очікується, що 5G підтримуватиме:

1. Пропускна здатність 10Mbps на квадратний метр у зонах гарячої точки.
2. Швидкість передачі даних, випробувана користувачем до 1 Гбіт/с, з піковими швидкостями передачі даних у десятках Гбіт/с і цілим обсягом трафіку не менше 1 Тбіт / с на квадратний кілометр.
3. Затримка в 1 мс для обміну даними з користувачами.
4. Щільність підключення до одного мільйона з'єднань на квадратний кілометр.

5. Висока мобільність до 500 км / годину в швидкісних поїздах і до 1000 км/годину в літаках.

Раннє використання можливостей eMBB зосереджується на споживчому ринку та необхідності кращого та швидшого підключення для обробки високоякісного відеоконтенту, збільшення кількості контенту, створеного користувачем, та наших очікувань можливості передавати те, що ми хочемо, куди хочемо та коли хочемо , без необхідності входити в мережу WiFi.

Але eMBB – це не лише споживання мультимедійного контенту для розважальних цілей. Він підтримуватиме маршрутний доступ до додатків із хмарних просторів на шляху до роботи, віддалених працівників на місцях, які потребують спілкування з бек-офісом, або ж із цілим розумним офісом, де всі пристрої підключені бездротово та безперебійно. Зрештою, це дозволить додаткам від повністю занурених VR та AR до відеоспостереження в режимі реального часу та віртуальних зустрічей з 360 відео, взаємодіяти в режимі реального часу та навіть можливості перекладу в реальному часі для учасників, які говорять на різних мовах.

Отже, надширокосмуговий мобільний зв'язок (eMBB) є послугою, що впроваджується спочатку на основі існуючих 4G мереж, а потім використовується технологією 5G. eMBB дозволяє збільшити швидкість передачі даних та збільшує пропускну здатність.

Література

1. 5G systems - Enabling the transformation of industry and society [<https://www.ericsson.com/en/reports-and-papers/white-papers/5g-systems--enabling-the-transformation-of-industry-and-society>].
2. What is 5G New Radio (5G NR) [<https://5g.co.uk/guides/what-is-5g-new-radio/>].
3. Мобильная связь на пути к 6G. Комплект в 2-х томах. 1225грн. Автор: Степутин А.Н., Николаев А.Д. Издательство: Инфра-Инженерия; Рік видання: 2017, с. 796. ISBN: 978-5-9729-0192-0.
4. What is enhanced Mobile Broadband (eMBB) / Sacha Kavanagh [<https://5g.co.uk/guides/what-is-enhanced-mobile-broadband-embb/>].

МЕТОД ПРОСТОРОВОГО ФОКУСУВАННЯ ЯК СПОСІБ ФОРМУВАННЯ ЕЛЕКТРОМАГНІТНИХ ХВИЛЬ ЗІ СФЕРИЧНИМИ ФАЗОВИМИ ФРОНТАМИ ДЛЯ ПІДВИЩЕННЯ ПРОДУКТИВНОСТІ РАДІОРЕЛЕЙНИХ ЛІНІЙ

Авдєєнко Г.Л., Якорнов Є.А.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського

E-mail: django2006@ukr.net

Spatial focusing method as a way for electromagnetic waves formation with spherical wavefronts for the bandwidth increase of microwave links

A mathematical model is developed and some simulation results for finding the electromagnetic energy focusing points which emitted by the elements of a linear sparse antenna array with spherical wavefronts in the space between corresponding microwave stations are obtained.

В роботі авторів [1] сформульовані ряд завдань по дослідженню можливостей використання відмінностей у формах фазових фронтів (ФФФ) електромагнітних хвиль (ЕМХ) для підвищення продуктивності радіорелейної лінії зв'язку (РРЛЗ) прямої видимості при знаходженні їх антенних систем в зоні Френеля і, зокрема, задача теоретичного аналізу можливості синтезу тієї чи іншої ФФФ ЕМХ шляхом суперпозиції випромінюваних антенами ЕМХ в певних точках простору (фокусах).

Розглянемо варіант вирішення цієї задачі для спрощеної схеми РРЛЗ з розрідженої антенної решітки (РАР), зображеної на рис.1, де РРС - радіорелейна станція, а ДУС - діаграмоутворююча схема, ПФ - просторовий фільтр.

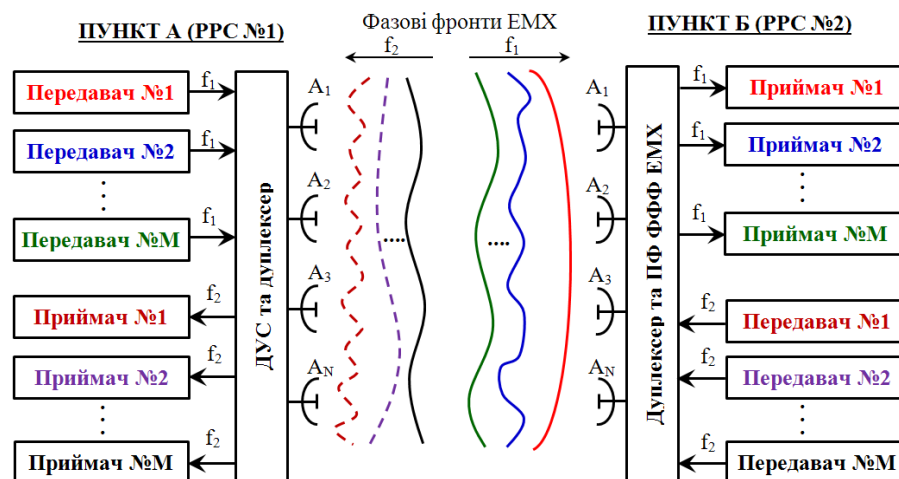


Рис.1. Спрощена схема РРЛЗ з на основі використання РАР.

За відсутності кривизни (сферичності) фронту ЕМХ кожен з N каналів передачі і прийому РРС може працювати автономно на парі частот $(f_{1i}, f_{2i}, i = \overline{1, N})$ як один дуплексний ствол або як два симплексні ствола.

При наявності кривизни фазового фронту ЕМХ, яка визначається довжиною інтервалу d між границями ближньої та далекої зони РАР РРС

$D_{БЗ} \ll d \ll D_{ДЗ}$ можливо здійснювати [1] просторову обробку сигналів по ФФФ на передачу і прийом на одній й тій самій несучій частоті f .

Оскільки в реальних РРЛЗ порядок величин d не перевищує декількох сотень метрів, то для збільшення інтервалу між РРС пропонується ввести процедуру вибору фокусів електромагнітної енергії (ЕМЕ), в яких хвили від РАР інтерферують синфазно і є вторинними джерелами випромінювання.

Для фокусування енергії від РАР в будь-яку точку ближньої або Френелівської зони випромінювання необхідно в кожному з k каналів передавальної РАР за допомогою керованих фазообертачів змінити фазу струму або за допомогою керованих ліній затримки внести часову затримку.

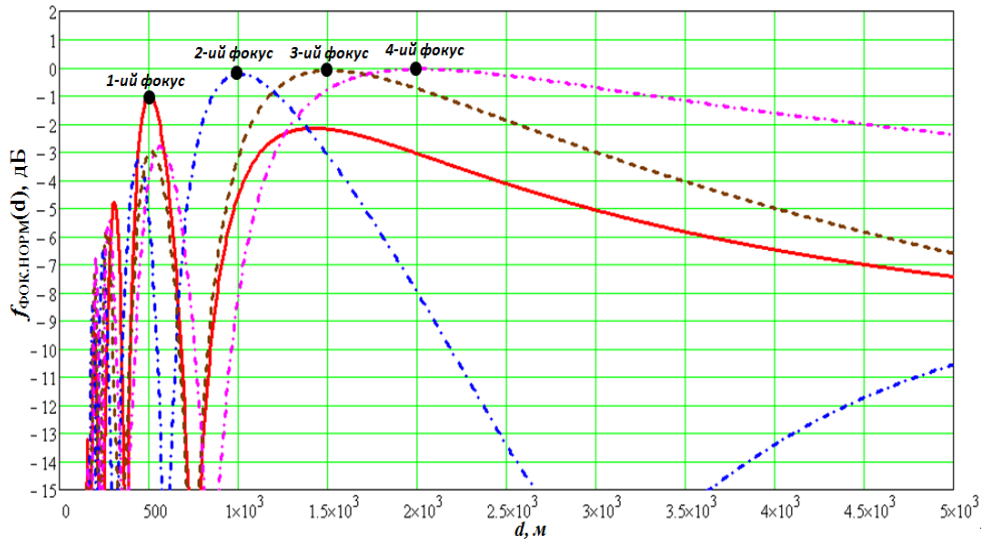


Рис.2. Просторовий розподіл положення фокусів.

Після фокусування ЕМЕ в деяку точку (рис. 2) вираз для сумарної напруженості поля в довільній точці простору (θ, d) може бути представлено у вигляді

$$\dot{E}_{\Sigma}(\theta, d) = \frac{A \dot{I}_m \exp(-j\beta d)}{d} \dot{f}_{.ББЗ.ФО}(\theta, d), \quad (1)$$

де A - множник, що залежить від типу антени (наприклад, для електричного вібратора $A = l\sqrt{\mu_a/\epsilon_a}/2\lambda$, де l - його довжина), I_m - максимальна амплітуда гармонійного струму в каналах РАР; $\beta = 2\pi/\lambda$;

$$\dot{f}_{.ББЗ.ФО}(\theta, d) = \sum_{k=1}^M F_{0пер}(\theta_k) \exp(-j\beta(d_k(\theta, d) - d)) \exp(j\Delta\varphi_{k0}(\theta_0, d_0)) = \mathbf{k}_{ФОК}^{*T} \mathbf{S}_a(\theta, d) -$$

характеристика спрямованості (ХС) сфокусованої в точку (θ_0, d_0) РАР;

$\mathbf{k}_{ФОК}^T = [\exp(j\Delta\varphi_{10}), \exp(j\Delta\varphi_{20}), \dots, \exp(j\Delta\varphi_{M0})]$ - вектор-стовпець вагових коефіцієнтів РАР, що описує встановлений з використанням фазообертаючих пристроїв фазовий розподіл поля в каналах передавальної РАР для фокусування поля в точку (θ_0, d_0) ;

$$\mathbf{S}(\theta, d) = \begin{bmatrix} F_{0пер}(\theta_1) \exp(-j\beta(d_1(\theta, d) - d)), F_{0пер}(\theta_2) \exp(-j\beta(d_2(\theta, d) - d)), \dots \\ \dots, F_{0пер}(\theta_M) \exp(-j\beta(d_M(\theta, d) - d)) \end{bmatrix}^T$$

- матриця розмірності $[M \times 1]$, так званий керуючий вектор РАР, що описує

амплітудно-фазовий розподіл струмів на розкритті передавальної РАР, які формують ЕМП в довільній точці простору з координатами (θ, d) .

Нормоване значення ХС РАР в фокусі ближньої зони

$$\dot{f}_{\text{БЗ.ФОК.НОРМ}}(\theta, d) = \frac{\mathbf{k}_{\text{ФОК}}^{*\text{T}} \mathbf{S}_a(\theta, d)}{M} = \frac{f_{\text{БЗ.ФОК}}(\theta, d)}{M}, \quad (2)$$

Якщо $d = d_0$, а $\theta = \theta_0$ то з (1) отримаємо, що в точці фокусування

$$\dot{f}_{\text{М.ФОК.НОРМ}}(\theta_0, d_0) = \frac{(1 + 1 + 1 + \dots + 1)}{M} F_{\text{0пер}}(\theta_0) = F_{\text{0пер}}(\theta_0), \quad (3)$$

Отриманий результат говорить про те, що установка фазових співвідношень в каналах РАР, описувана вектором фокусування $\mathbf{k}_{\text{ФОК}}$, призводить до вирівнювання фази (часових затримок) гармонійних радіосигналів від різних антенних елементів в точці фокусування $F(\theta_0, d_0)$, яка обумовлена різними відстанями до неї, внаслідок чого напруженості ЕМП від різних антенних елементів складаються в точці фокусування $F(\theta_0, d_0)$ синфазно.

Умова фокусування сигналів, що приходять в точку F від антен A_1, A_2, A_3 при $\theta = 0^\circ$ і $d_2 = D$ може бути записана як

$$d_1 - D = d_3 - D = n\lambda, \quad n = 0 \dots \infty, \quad n \in Z \quad (4)$$

чи

$$\Delta\varphi_{12} = \Delta\varphi_{32} = \beta(d_1 - D) = \beta(d_3 - D) = 2\pi n. \quad (5)$$

Враховуючи, що $d_1 = d_3 = \sqrt{L_1^2 + D^2}$, отримаємо, що координати точок фокусування

$$D(n) = \frac{(K^2 - n^2)\lambda}{2n}, \quad (6)$$

де $K = L_1/\lambda$ – відношення розмірів бази РАР до довжини хвилі.

Таким чином, згідно з (6) 3-х елементна РАР має K фокусів, з яких два фокуси, для яких $n = K$ и $n = 0$ відповідають точці розташування антени A_2 і нескінченності (дальній зоні).

Таким чином, виходячи з аналізу умов поширення хвиль, відстаней між прольотами РРС і потоку інформації, що передається, оператор(и) може відповідно до співвідношення (6) шляхом зміни фазового зсуву $\Delta\varphi_{10}$ підбирати точки фокусування ЕМЕ від декількох елементів РАР на лінії, для налаштування на необхідну дальність між РРС і регулювання кривизни того чи іншого фазового фронту ЕМХ. Схемна реалізація даного методу показана в [2].

Література

1. Авдеенко Г.Л., Якорнов Е.А. Задачи практической реализации радиорелейной линии связи на основе использования различий в формах фазовых фронтов их электромагнитных волн //XI Міжнародна науково-технічна конференція "Проблеми телекомунікацій" ПТ-2017: Збірник матеріалів конференції. К.: КПІ ім. Ігоря Сікорського, 2017. – с.235-237.
2. Декларативний патент на корисну модель № 140040 (Україна). Система забезпечення зв'язку між двома радіорелейними станціями, кл. Н04В7/14 //Авдеєнко Г.Л., Лільченко М.Ю., Якорнов Є. А. та інш. - Промисл. власність, 2020, № 3.

ОЦІНКА ЕНЕРГЕТИЧНОГО ПОТЕНЦІАЛУ ДЛЯ ЛІНІЇ РАДІОЗВ'ЯЗКУ «ТОЧКА-ТОЧКА» НА БАЗІ ТРАНСИВЕРІВ DWM 1000

Денисенко Н. І., Авдєєнко Г. Л.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: natalka.denysenko@gmail.com

Evaluation of energy potential for a point-to-point radio link based on the DWM 1000 transceivers

Block diagram of a «PtP» duplex link based on the DWM 1000 transceivers was developed. The dependence of information transmission distance was determined at different data rates with maximum allowable losses.

Трансивер DWM1000, який виготовляє компанія DecaWave, що відповідає специфікації стандарту IEEE 802.15.4-2011 оптимізований для застосувань у системах локального позиціонування в реальному часі та бездротових сенсорних мережах, включаючи мережу IoT, сільське господарство, управління будівництвом, охорону здоров'я, безпеку, логістику та ряд інших[1]. Специфікою даного трансиверу є використання надширококутових сигналів.

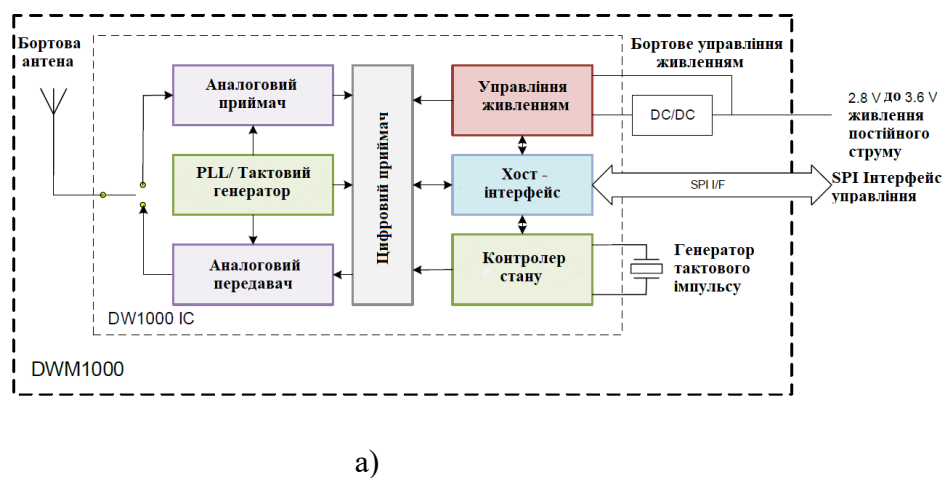


Рис.1. UWB трансивер DWM1000: (а) структурна схема трансиверу, (б) фотографія трансиверу.

Структурну схему безпроводової лінії зв'язку «точка-точка» на базі трансиверу DWM1000 наведено на рис. 2.

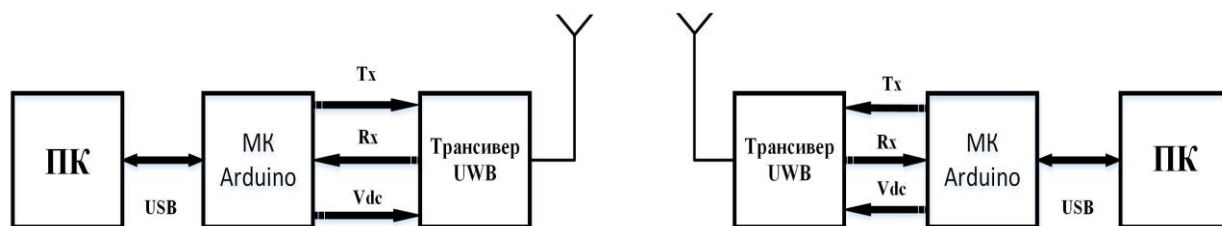


Рис.2. Структурна схема дуплексної системи зв'язку типу «PtP».

Для вище зазначеної схеми було виконано наступні розрахунки залежності відстані між станціями в радіоканалі від швидкості передачі. Вихідні дані для розрахунку наведено в таблиці 1 та 2.

Таблиця 1. Вихідні дані для проведення енергетичного розрахунку.

Ширина спектру випромінювання	Спектральна щільність потужності	Коефіцієнт підсилення антени	Центральна частота	Довжина хвилі
$\Delta f = 900 \text{ МГц}$	$P_{\text{пер min}} = -62 \text{ дБм/МГц}$ $P_{\text{пер max}} = -35 \text{ дБм/МГц}$	$G_{\text{пр}} = -5 \text{ дБі}$ $G_{\text{пер}} = -5 \text{ дБі}$	$f = 3993.6 \text{ МГц}$	$\lambda = 0.75 \text{ м}$

Таблиця 2. DWM1000 Типові характеристики чутливості приймача [2].

PER	Швидкість передачі даних	Чутливість приймача	Одиниці виміру	Умова / Примітка	
1%	110 кбіт/с	-102	дБм/ 500 МГц	Преамбула 2048	Всі вимірювання, проведені на 5 каналі PRF 16МГц. Канал 2 приблизно на 1 дБ менш чутливий.
	850 кбіт/с	-101	дБм/ 500 МГц	Преамбула 1024	
	6,8 мбіт/с	-93	дБм/ 500 МГц	Преамбула 256	
10%	110 кбіт/с	-106	дБм/ 500 МГц	Преамбула 2048	
	850 кбіт/с	-102	дБм/ 500 МГц	Преамбула 1024	
	6,8 мбіт/с	-94	дБм/ 500 МГц	Преамбула 256	

Методика розрахунку залежності відстані між станціями від швидкості передачі даних:

1. Задаємо спектральну щільність потужності $P_{\text{пер min}}$ ($P_{\text{пер max}}$).
2. Додаємо до спектральної щільності потужності $P_{\text{пер min}}$ ($P_{\text{пер max}}$) $10 \lg \Delta f^{\text{[МГц]}}$, де ширина спектру випромінювання $\Delta f = 900 \text{ МГц}$.
3. Вибираємо мінімальну швидкість передачі даних $V_{\text{min}} = 110 \text{ кбіт/с}$ та $\text{PER} = 1\%$.
4. Визначаємо чутливість приймача $P_{\text{спрм min}}$ (при ширині спектрального випромінювання $\Delta f = 500 \text{ МГц}$ (з табл. 2) для вибраної мінімальної швидкості передачі даних V_{min}).
5. Перераховуємо чутливість приймача $P_{\text{спрм}}$ для ширини спектрального випромінювання $\Delta f = 900 \text{ МГц}$. За формулою:

$$P_{\text{спрм} \Delta f = 900 \text{ МГц}}^{\text{[дБм]}} = P_{\text{спрм} \Delta f = 500 \text{ МГц}}^{\text{[дБм]}} + 10 \lg \frac{900}{500} \quad (1)$$

6. Розраховуємо максимально допустимі втрати в радіоканалі для каналу. За формулою:

$$L^{\text{[дБм]}} = P_{\text{пер}}^{\text{[дБм]}} + G_{\text{пер}}^{\text{[дБм]}} + G_{\text{пр}}^{\text{[дБм]}} - P_{\text{спрм}}^{\text{[дБм]}} \quad (2)$$

7. Визначаємо дальність із формули:

$$L = 20 \lg \frac{4\pi d}{\lambda} \quad (3)$$

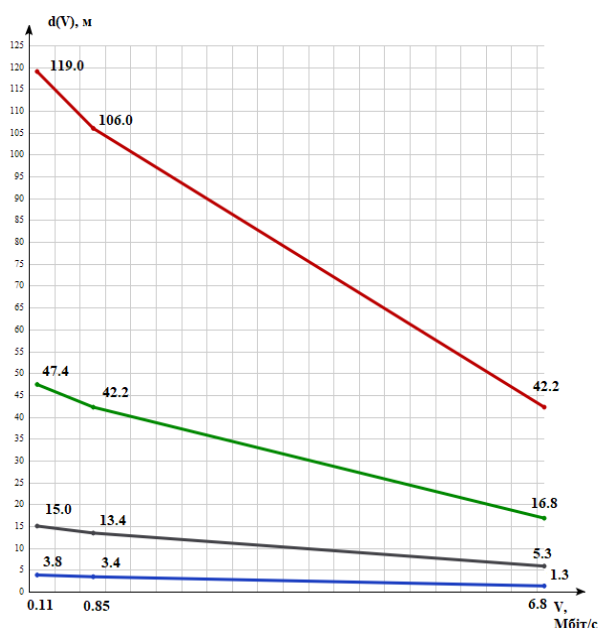
Результати вирішення рівнянь (1–3) представлено в табл.3 та табл.4.

Таблиця 3. Результати розрахунку втрат в радіоканалі при різній спектральній щільності потужності.

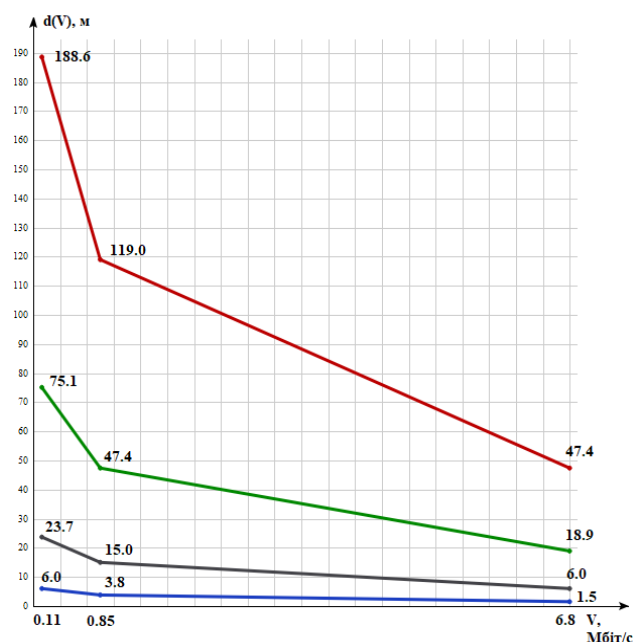
L, дБ P _{пер} дБм/МГц	L(PER=1%) 2-ий канал			L(PER=10%) 2-ий канал		
P _{пер} = -62	55.99	54.99	46.99	60.99	59.99	51.99
P _{пер} = -50	67.99	66.99	58.99	72.99	71.99	63.99
P _{пер} = -40	77.99	76.99	68.99	82.99	81.99	73.99
P _{пер} = -32	85.99	84.99	76.99	90.99	89.99	81.99

Таблиця 4. Результати розрахунку відстані між станціями в радіоканалі в залежності від швидкості передачі.

d(м) при L(PER=1%)			d(м) при L(PER=10%)		
V=110 Кбіт/с	V=850 Кбіт/с	V=6.8 Мбіт/с	V=110 Кбіт/с	V=850 Кбіт/с	V=6.8 Мбіт/с
3.8	3.4	1.3	6.0	3.8	1.5
15.0	13.4	5.3	23.7	15.0	6.0
47.4	42.2	16.8	75.1	47.4	18.9
119.0	106.0	42.2	188.6	119.0	47.4



а)



б)

Рис. 3. Графіки залежності відстані між станціями від швидкості передачі даних $d=f(V)$ при максимально допустимих втратах у радіоканалі: а) при PER=1%; б) при PER=10%.

На основі виконаних розрахунків можна зробити висновки, що чим менша швидкість передачі даних, тим більші максимально допустимі втрати й тим більша відстань між станціями, при збільшенні швидкості – навпаки. Дане явище повністю відповідає класичній Шеннонівській теорії інформації.

Література

1. PRODUCT INFORMATION: DWM1000 [Електронний ресурс] – Режим доступу до ресурсу: <https://www.decawave.com/>.
2. DW1000 Datasheet [Електронний ресурс] // Version 2.19 – Режим доступу до ресурсу: <https://www.decawave.com/>.

ПРОБЛЕМИ ПРОЕКТУВАННЯ ПРИЛАДІВ ДЛЯ МЕРЕЖ 5G МІЛІМЕТРОВОГО ДІАПАЗОНУ

Свіржевська А. І.

Інститут телекомунікаційних систем КПП ім. Ігоря Сікорського, Україна

E-mail: angelina.svirzhevskaya@gmail.com

Problems of designing devices for 5g millimeter networks

Designing devices for 5G millimeter networks requires a compromise between a number of parameters and characteristics.

Область міліметрових хвиль добре зарекомендувала себе в «розумних» автомобільних системах, а можливість забезпечити робочу смугу від 30 до 300 ГГц є дуже перспективним напрямком, особливо в порівнянні з мережами LTE. Проте побудова мереж 5G, що використовують всі переваги міліметрового діапазону, вимагає збільшення рівнів потужності переданих сигналів, а це значить, що ключову роль у розвитку нових систем буде грати доступність відповідних підсилювачів потужності (ПП).

Сучасні мережі орієнтовані на передачу великих обсягів даних, що, відповідно, вимагає великої швидкості передачі даних та пропускної здатності мереж. Поява і розвиток Інтернету речей (IoT) також веде до створення пристроїв з низьким енергоспоживанням, оскільки велика їх частина постійно знаходиться у включеному стані з безперервним бездротовим підключенням до інтернету. Це відрізняє пристрої IoT від смартфонів, які можуть перебувати в режимі очікування без постійного споживання ресурсів мережі. За різними оцінками, кількість пристроїв IoT, які повинні будуть знаходитися в підключеному до мережі стані, може досягати декількох трильйонів вже через кілька років - при цьому не враховується зростання кількості смартфонів, що працюють в тих же мережах. У зв'язку з цим необхідність в мережах з високою пропускною спроможністю стає нагальною проблемою.

Пропускна здатність мережі залежить від ряду факторів, що включають доступну смугу, кількість каналів зв'язку, кількість сот і відношення сигнал / шум. Збільшення робочої смуги за рахунок переходу в міліметрову область

спектра дозволить підвищити пропускну здатність, однак при цьому розробники сподіваються уникнути серйозного збільшення енергоспоживання, що є важливою вимогою до проектування ПП для 5G не тільки на високих, але і на відносно низьких частотах.

Як правило, ПП описується рядом характеристик, серед яких - коефіцієнт підсилення, стабільність підсилення, рівень вихідної потужності, лінійність, ККД, вхідний і вихідний коефіцієнти стоячої хвилі по напрузі (КСХН) і коефіцієнт шуму. Робоча смуга конкретного ПП визначається здатністю підсилювача зберігати значення цих параметрів в необхідному діапазоні.

Проектування підсилювача для мереж 5G міліметрового діапазону вимагає досягнення компромісу між рядом параметрів і характеристик, а особливо лінійності і ККД. Висока лінійність більшості ПП досягається при роботі на рівнях потужності вхідного сигналу нижче максимального - таким чином ПП не переходить в режим компресії. З іншого боку, ККД підсилювачів максимальний при роботі саме в режимі компресії, а саме в точці, де режим роботи ПП вважається насиченим і його вихідна потужність максимальна, оскільки подальше збільшення вхідного сигналу не приведе до істотного збільшення вихідної потужності. Високий ККД необхідний для мінімізації споживання електроенергії базової станції або мікростільника. Аналогічно підсилювачі в мобільних пристроях, що працюють від батарей, повинні працювати в лінійному режимі без шкоди значенням ККД по доданій потужності.

Для забезпечення високої лінійності ПП при збереженні достатнього ККД часто використовуються методи цифрової корекції передспотворень. Оскільки підсилювач володіє найбільшим ККД в області точки насичення, цифрова корекція дозволяє змінювати форму модульованих сигналів таким чином, щоб він працював з високим ККД, але без спотворень або підвищеної нелінійності.

Залежно від технології активного пристрою типовою є задача вибору конструкції підсилювача, кількості каскадів і т.д. Кінцевий результат буде

визначатися набором вимог до підсилювача: частотний діапазон, коефіцієнт посилення, вихідна потужність, лінійність і ККД.

Отримання оптимальних характеристик залежить від якості рішення задачі узгодження вхідного і вихідного імпедансу транзистора до характеристичного імпедансу системи. Як правило, з цією метою проводять виміри S-параметрів пристрою на векторному аналізаторі для отримання малосигнальних характеристик на вході, а також load-pull-вимірювання за допомогою відповідного тюнера для нелінійного узгодження вихідного імпедансу на основі даних, отриманих в режимі великого сигналу. Оптимальний імпеданс джерела дозволяє зменшити коефіцієнт шуму ПП, в той час як узгодження навантаження необхідно для отримання необхідних параметрів вихідної потужності, ККД і лінійності.

Залежно від конкретного застосування (стаціонарного або портативного) підсилювач для мереж 5G повинен відповідати різним вимогам до частотного діапазону, рівня потужності, ККД і лінійності. Стандартні лінійні симуляції дозволяють оцінити коефіцієнт підсилення, поворотні втрати та інші параметри в залежності від частоти.

Незважаючи на те, що міліметровий діапазон частот може забезпечити дуже широкі робочі смуги для пристроїв мереж 5-го покоління і інших застосувань, включаючи автомобільні радари і системи безпеки, підсилювачі потужності для цих областей, ймовірно, будуть обмежені в робочій смузі. Багато організацій, які планують введення мереж 5G, пропонують використання вузьких каналів передачі даних навколо центральних частот 24, 28 або 60 ГГц. Крім цього, проектування узгоджувальних схем у вузькій смузі значно простіше, ніж в широкій, особливо в тому випадку, якщо мова йде про пристрої, що працюють в міліметровому діапазоні хвиль.

Література

1. <https://digital.gov.ru/uploaded/files/proekt-kontseptsii-sozdaniya-i-razvitiya-setej-5g-imt-2020-v-rossijskoj-federatsii.pdf>.
2. <https://www.analog.com/ru/landing-pages/001/national-instruments.html#>.
3. https://niir.ru/wp-content/uploads/2018/12/ES-12_butenko.pdf.

АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ ПРИСТРОЇВ ТА ПОСЛУГ ІНТЕРНЕТУ РЕЧЕЙ

Піхота К.В., Кононова І.В.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: pihotka19.11@gmail.com

Analysis of security threats to Internet of Things devices and services

The main weaknesses in building the Internet of Things were identified by analyzing major technology threats and providing recommendations (comprehensive security measures) to improve the security of Internet of Things devices and services.

На даний час спостерігається швидкий темп росту пристроїв Інтернету речей, який надає безліч переваг, однак пристрої IoT (internet of things - інтернет речей) можуть надавати реальну загрозу безпеці, тим більше що вони можуть бути легко скомпрометовані і можуть привести до більш серйозних порушень, видалення, спотворення даних і інших проблем.

Експоненціальне зростання IoT призвело до збільшення ризиків для безпеки та конфіденційності. Багато таких ризиків можна віднести до вразливості пристроїв, які виникають внаслідок кіберзлочинності хакерами та неправильного використання системних ресурсів.

Беручи до уваги дослідження, що провела в 2019 компанія Microsoft, яке присвячувалось динаміці впровадження Інтернету речей в компаніях з різних індустрій і країн світу 85% організацій вже мають як мінімум один бізнес-проект в цій сфері, а до 2021 року ця цифра виросте до 94%. При цьому 88% керівників таких проектів усвідомлюють переваги технології для успіху компанії і очікують 30% окупність інвестицій в дворічній перспективі [1].

Тому, необхідно проаналізувати загрози безпеки та визначимо основні проблеми з пристроями і послугами IoT.

Безпека даних являє собою фундаментальну проблему в пристроях і послугах IoT [2]. В контексті IoT доступ до даних може мати не тільки користувач, але і авторизований об'єкт. Це вимагає розгляду двох важливих аспектів: по-перше, механізму контролю доступу та авторизації та другого механізму аутентифікації і управління. Пристрій IoT повинні перевірити, що об'єкт (людина або інший пристрій) авторизований для доступу до послуги. Авторизація допомагає визначити, чи дозволено при ідентифікації об'єкту отримувати послугу. Контроль доступу є невід'ємною частиною контролю доступу до ресурсів шляхом надання або відмови в засобах надання послуг з використанням широкого набору критеріїв.

Авторизація та контроль доступу необхідні для встановлення безпечного з'єднання між кількома пристроями та службами. Основною проблемою в цьому сценарії є спрощення створення, розуміння і маніпулювання правилами контролю доступу, а також слід враховувати при роботі з конфіденційністю: аутентифікацію та управління ідентифікацією, оскільки кільком об'єктам розпізнавати один одного за допомогою надійних служб ця проблема є критичною в IoT.

В проведених дослідженнях, вченими та передовими компаніями, основна увага приділяється безпеці з погляду конфіденційності, що є важливою проблемою для пристроїв і послуг IoT з погляду на те, що об'єкти пов'язані між собою, а дані передаються та обмінюються через Інтернет. Тому, довіра грає важливу роль у встановленні безпечного з'єднання у невизначеному середовищі IoT [3]. На даний час слід розглядати два аспекти довіри: довіра до взаємодій між об'єктами і довіра до системи з точки зору користувачів. Надійність пристроїв IoT, найчастіше, залежить від компонентів пристрою, включаючи обладнання (процесор, пам'ять, датчики) і виконавчі механізми, програмні ресурси (апаратне програмне забезпечення, операційна система, драйвери та додатки, а також джерело живлення). Отже, для підвищення надійності пристроїв повинен існувати ефективний механізм визначення довіри в спільному середовищі IoT.

Розглянемо вплив на цілісність системи з погляду підвищення надійності технології IoT.

Перед усуненням загроз безпеки необхідно спочатку ідентифікувати системні ресурси, які складають IoT, при цьому необхідно розуміти інвентаризацію активів, включаючи всі компоненти IoT, обладнання та послуги, що надаються [4].

Основними активами будь-якої системи IoT є системне устаткування (включаючи будівлі, обладнання і т.д.) , програмне забезпечення, послуги і дані, які пропонуються цими послугами. Виходячи з активів системи, можна класифікувати вплив на цілісність системи, за такими показниками як вразливість, вплив та загроза.

Під вразливістю розуміється слабкі місця в системі або її структурі, які дозволяють зловмиснику виконувати команди, несанкціоновано отримувати доступ до даних і/або проводити атаки типу «відмова в обслуговуванні». Вразливості можуть бути виявлені в різних областях систем IoT, це можуть бути слабкі місця в системному обладнанні або програмному забезпеченні, слабкі місця в політиках і процедурах, використовуваних в системах, а також слабкі сторони самих користувачів системи.

Показник «вплив» в IoT є проблемою або помилкою в конфігурації системи, що дозволяє зловмиснику виконувати дії зі збору інформації. У більшості додатків IoT пристрій може залишитись без нагляду або бути

розміщеним в легко доступному для зломисників, що може стати важливою проблемою - фізичною атакою, наприклад, пошкодження криптографічних даних, перепрограмування компонент або заміна їх шкідливим пристроєм [5].

Також на цілісність системи впливає показник «загроза» [6]. Загрози можуть виникати з двох основних джерел: люди і природа.

Розглянувши основні проблеми безпеки пристроїв та служб IoT, можна зробити висновок, що вони піддаються ряду поширених загроз, наприклад, віруси та атаки відмови в обслуговуванні і проведення простих заходів для уникнення таких загроз та подолання вразливості системи недостатньо. Таким чином, необхідно забезпечити безперервний процес реалізації політики, що буде підтримуватися суворими процедурами.

Процес розробки безпеки вимагає глибокого розуміння активів системи з подальшим виявленням різних вразливостей та загроз, які можуть існувати.

Необхідно визначити, що таке активи системи та від чого активи повинні бути захищені. У роботі активи визначені як усі цінні речі в системі, матеріальні та нематеріальні, які потребують захисту. Деякі загальні активи IoT включають системне обладнання, програмне забезпечення, дані та інформацію, а також активи, пов'язані з послугами. Розуміння потенційних атак дозволить розробникам системи краще визначати, на що слід звернути більше уваги для забезпечення коректної та безпечної роботи системи.

Отже, для уникнення ризиків для безпеки та конфіденційності, IoT має бути побудований таким чином, щоб забезпечити простий та безпечний контроль використання, а для цього в першу чергу необхідно забезпечити захист пристроїв і послуг IoT від несанкціонованого доступу як всередині пристроїв, так і ззовні.

Література

1. Интернет вещей, IoT, M2M (мировой_рынок). – Электронный ресурс. – Режим доступа: [http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9,_IoT,_M2M_\(%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%BE%D0%B9_%D1%80%D1%8B%D0%BD%D0%BE%D0%BA\)](http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9,_IoT,_M2M_(%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%BE%D0%B9_%D1%80%D1%8B%D0%BD%D0%BE%D0%BA)).
2. D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges".
3. M. Abomhara and G. Koien, "Security and privacy in the internet of things: Current status and open issues".
4. D. Watts, "Security and vulnerability in electric power systems".
5. D. G. Padmavathi, M. Shanmugapriya et al., "A survey of attacks, security mechanisms and challenges in wireless sensor networks," arXiv preprint arXiv:0909.0576, 2009.
6. H. G. Brauch, "Concepts of security threats, challenges, vulnerabilities and risks," in Coping with Global Environmental Change, Disasters and Security. Springer, 2011, pp. 61–106.

ІНКУБАТОР ДЛЯ ЯЄЦЬ З ТЕХНОЛОГІЄЮ INTERNET OF THING

Губар В.Г., Якименко О.О.

Факультет електроніки КПІ ім. Ігоря Сікорського

E-mail: o.yakymenko22@gmail.com, s.gubar@kpi.ua

Eggs incubator with internet of things technology

Almost all existing incubators do not have remote control, notifications of emergency and possibility of creation incubation program. But these functions are extremely important for incubation. Upgrading incubator with IoT technology resolves all problems and extends incubator's functionality.

Інкубаційний період перепелиних яєць складає близько 17 днів [1]. Зі збільшенням розмірів яєць час інкубації теж збільшується [1]. У випадку, якщо жодним чином не реалізоване автоматичне керування інкубатором, впродовж всього часу інкубації, фермеру потрібно кожного дня особисто контролювати процес. У випадку виникнення надзвичайних ситуацій, без сповіщень, фермер не зможе оперативно реагувати на події, що може призвести до значних збитків.

Іншою проблемою є універсалізація. Зазвичай, у господарстві фермер має декілька видів тварин. І робити окремі покупки інкубаторів для різних тварин є економічно не вигідним та не рентабельним. Не кажучи вже про екзотичні тварини - такі як змії чи крокодили.

Для успішної інкубації, інкубатор має підтримувати встановлену температуру, вологість, робити періодичний поворот яєць та забезпечувати циркуляцію повітря. Але, якщо в інкубатор вбудувати підтримку Інтернету Речей (Internet of Things), то можливості інкубатору значно розширюються і він вже може забезпечити такі вимоги:

- Віддалений контроль та керування;
- Сповіщення у Telegram або на пошту у випадку надзвичайних ситуацій та по закінченню інкубації;
- Створення погодинних програм інкубації для будь-яких тварин;
- Використання вже створених програм інкубації.

Після аналізу ринку, а саме, відомих сайтів таких як Amazon, AliExpress, було виявлено, що з базовими можливостями є безліч моделей інкубаторів різного класу. З функцією IoT було знайдено лише блок керування однієї моделі [2], але без можливості створення програм інкубації. Готового рішення інкубатору знайдено не було.

При розробці експериментального зразку інкубатору слід в першу чергу звернути увагу на підтримку умов мікроклімату.

Для вимірювання температури і вологості було використано точний

датчик SHT30 [4]. У якості нагрівального елементу було використано два малопотужні керамічні елементи [5]. Стабільність температури забезпечується за допомогою алгоритму ПД [3] регулятора. Підбір коефіцієнтів для забезпечення правильної роботи відбувався за допомогою методу Циглера-Нікольса [3].

Для підтримки вологості використовується ультразвуковий зволожувач [6] повітря.

Для розрахунку часу роботи зволожувача для випаровування певної маси води використаємо формули наведені нижче:

$$t = \frac{\Delta m}{r},$$

де t – час, час роботи випаровувача

Δm - маса води, яку необхідно випарувати

r – витрати води ультразвукового випаровувача в мл/год

$$\Delta m = \frac{V * \rho_0}{100} * (\varphi_{\text{бажане}} - \varphi_{\text{теперішнє}}),$$

де V – об'єм інкубатора

ρ_0 – густина насиченого пару

$\varphi_{\text{бажане}}$ – вологість, яку необхідно отримати

$\varphi_{\text{теперішнє}}$ – нинішня вологість в інкубаторі

Для встановлення інтернет з'єднання було обрано Skylab SKW92B[7]. Це простий одноплатний мікрокомп'ютер, на якому реалізовано роботу спеціалізованого для мережеских рішень дистрибутиву Linux під назвою openWRT[8]. На відмінну від SoC ESP8266, даний модуль дає можливість використовувати для програмування високорівневі мови програмування, такі як Python. Це в свою чергу дає змогу впровадити повністю асинхронний обмін даними з сервером за допомогою Python реалізації технології WebSocket.

Обмін даними між мікрокомп'ютером та мікроконтролером відбувається за допомогою протоколу UART(universal asynchronous receiver-transmitter).

Програма інкубації зберігається в постійній пам'яті мікроконтролера.

Інформація про стан системи впродовж всього періоду інкубації зберігається як в постійній пам'яті на мікрокомп'ютері локально так і в базі даних на сервері. Це дає змогу у випадку зникнення WI-FI не втратити інформацію та при відновленні зв'язку синхронізувати локальну базу даних з базою даних на сервері.

Написання програм інкубації відбувається в спеціальному інтерфейсі в особистому кабінеті на сайті. Завантажується програма в інкубатор в момент, коли забажає користувач. За бажанням фермер також має можливість

завантажувати сторонні програми інкубації. Таким чином фахівці з інкубації зможуть зробити свою науково обґрунтовану програму інкубації та надати її в публічний доступ. Це дасть змогу збільшити ефективність інкубації.

Крім сайту, як інтерфейс до інкубатору також виступає Telegram бот. Інформацію про стан інкубатору можна отримати за допомогою простих запитів в додатку Telegram.

Впродовж інкубації сервер періодично відправляє до інкубатора тестові повідомлення. Таким чином, у випадку, якщо відбудеться надзвичайна ситуація, вона реєструється на сервері та відбудеться негайне сповіщення за допомогою Telegram.

У випадку, якщо WI-FI мережа недоступна, то для управління інкубатор створює власну точку доступу до якої може підключитись користувач. У випадку надзвичайної ситуації сповіщення будуть надходити за допомогою каналу зв'язку мобільних телефонів GSM(Global System for Mobile Communications) методом відправки SMS(short message service) повідомлень користувачу.

Підсумувавши, впровадження IoT технології в інкубатор значно змінило процес інкубації. Можливість отримати інформацію про стан інкубації з будь-якого місця, значно зекономить час фермерів. Миттєві сповіщення в будь-який момент часу про можливу проблему, значно збільшує надійність інкубації та звільняє фермера від особистого постійного контролю за процесом. Зручне створення програм інкубації на смартфоні чи комп'ютері збільшує універсалізацію інкубатора для будь-яких тварин, навіть специфічних. Та звільняє фермера від періодичної ручної зміни умов інкубації.

Література

1. Інкубація різних видів птиць.
URL: <https://good-tips.pro/index.php/farm/poultry/incubation-of-eggs-different-types-of-poultry-in-one-incubator>(дата звернення: 15.03.2020).
2. Блок керування WI-FI інкубатору.
URL:https://www.amazon.com/UKSAT-Incubator-Controller-Temperature-Intelligent/dp/B0861WWNRR/ref=sr_1_2?dchild=1&keywords=eggs+incubator+wi-fi&qid=1584794111&sr=8-2(дата звернення: 20.02.2020).
3. ПІД контролер.
URL: https://en.wikipedia.org/wiki/PID_controller(дата звернення: 20.03.2020).
4. Датчик температури та води.
URL: <https://cutt.ly/pthusuJ>(дата звернення: 20.03.2020).
5. Нагрівальні елементи інкубатора.
URL: <https://cutt.ly/athyTAB>(дата звернення: 20.03.2020).
6. Ультразвуковий зволожувач повітря.
URL: <https://en.wikipedia.org/wiki/Humidifier> (дата звернення: 20.03.2020).
7. Одноплатний комп'ютер Skylab SKW92B.
URL: <http://www.skylabmodule.com/skw92b/> (дата звернення: 20.03.2020).
8. Дистрибутив Linux openWRT.
URL: <https://en.wikipedia.org/wiki/OpenWrt> (дата звернення: 20.03.2020).

ДИСТАНЦІЙНО-ПРОГРАМОВАНИЙ КОНТРОЛЕР ДАТЧИКІВ ТА ПРИСТРОЇВ

Сергієнко А.В., Губар В.Г.

Факультет електроніки КПІ ім. Ігоря Сікорського, Україна

E-mail: artur.serhiienko@gmail.com, s.gubar@kpi.ua

Remotely programmable controller of sensors and devices

Investigated the complexity of present-day smart home systems and how they affect the humanity. Presented universal system of smart house which is implemented by using external API of Telegram.

Досліджено складність сучасних систем розумного будинку та їх вплив на людство. Представлена універсальна система розумного будинку, яка реалізована за допомогою Telegram API.

Розвиток технологій спричинив виникнення нових пристроїв, які в свою чергу полегшують життя людей по всьому світу. Побутові прилади, економні світлодіодні лампи, твердопаливні котли, системи поливу, тощо. Загалом, для контролю та керування, техніка вимагає безпосередньої взаємодії з людиною. Вирішенням даної проблеми стало застосування систем дистанційного керування та контролю. Одним з найрозповсюдженіших типів таких систем є система «розумного будинку» [1]. До такої системи можна підключити електронні пристрої та виконувати дистанційне керування за допомогою виділеної панелі управління або додатку на смартфоні. Спектр застосування систем «розумного будинку» доволі широкий. Запропоновані ринком позиції можуть виступати одночасно як охоронні системи, системи контролю за освітленням та повітрям та навіть нагадувати про оплату комунальних послуг.

Системи «розумного будинку» є складними програмно-апаратними комплексами. Універсальність систем «розумного будинку» залежить від гнучкості програмних та схемо-технічних рішень. Розробка таких систем потребує великої кількості ресурсів та часу, що впливає на зростання ціни кінцевого продукту. Виходом з положення може стати, якщо використати за основу сторонні систем з відкритими програмними та апаратними інтерфейсами.

Враховавши складність реалізації, вирішено розробити подібну систему «розумного дому», яка розрахована на креативних користувачів. Користувач власноруч зможе під'єднати пристрій або датчик до системи та встановити

логіку роботи підключеного компоненту системи за допомогою соціальної мережі Telegram [2].

Telegram – розповсюджений додаток, що дозволяє обмінюватись текстовими повідомленнями SMS (Short Message Service), аудіо- та відеоматеріалами, тощо. Месенджер надає можливість створення облікового запису, за допомогою якого будуть автоматично оброблятися та відправлятися повідомлення. Такий обліковий запис називається – бот. Логіка бота контролюється за допомогою HTTPS запитів до безкоштовного інтерфейсу програмування додатків – API. Для здешевлення кінцевого продукту, інтерфейсом управління та програмування виступає Telegram бот [3]. Приклад використання системи можна переглянути нижче на рис 1.

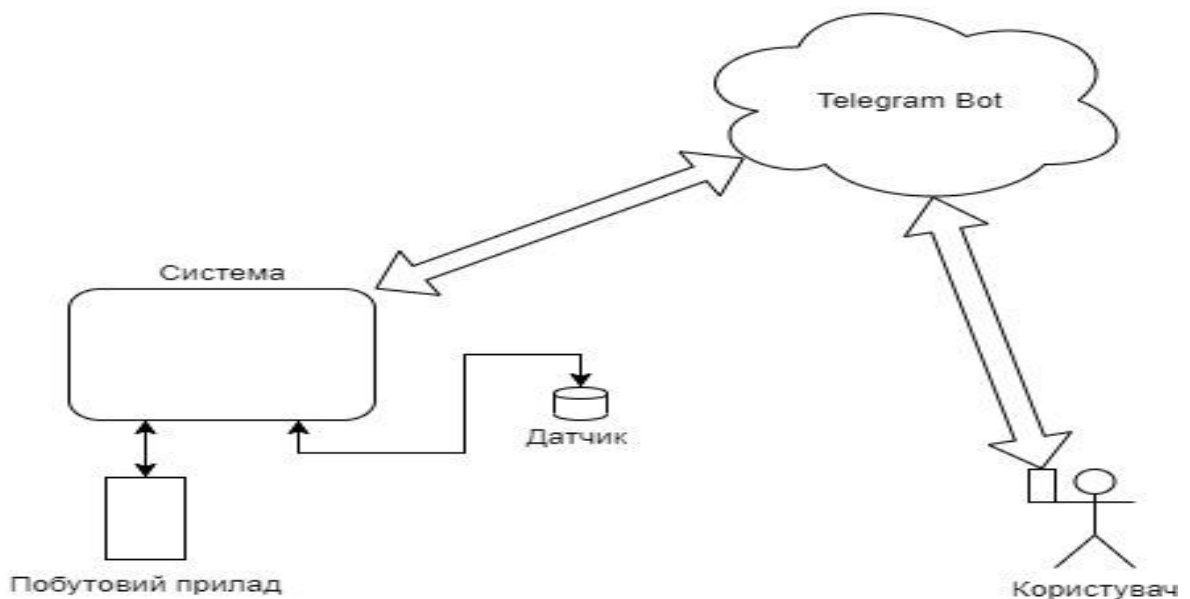


Рис. 1. Функціональна схема системи

Для даної системи можна виокремити такі особливості :

- Можливість швидкого розширення функціональних можливостей;
- Відносна простота розробки;
- Легкість керування та налаштування користувачем;
- Універсальність.

Розглянемо структурну схему системи на рис 2.

За блок сповіщення та блок введення даних відповідає Telegram. Користувач налаштовує логіку системи, використовуючи інтерфейс Telegram бота. Якщо користувач хоче отримувати сповіщення про подію, пов'язану зі зміною стану в системі, він має змогу також це налаштувати.

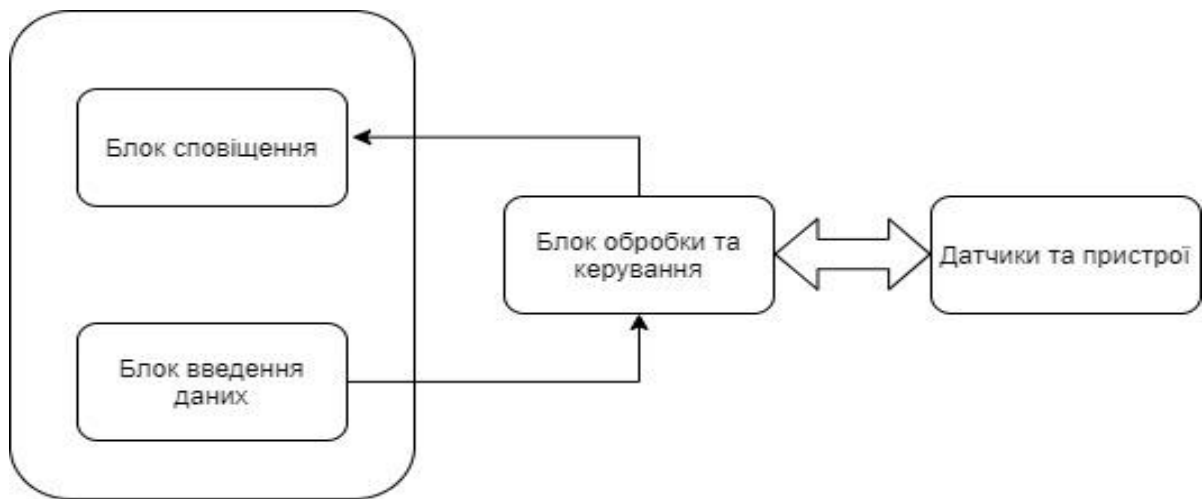


Рис. 2. Структурна схема системи

Блок обробки та керування. За обробку та керування, відповідає одноплатний мікрокомп'ютер NanoPi Neo 2 [4]. Даний мікрокомп'ютер може підтримувати дистрибутиви операційної системи Linux, можливість дротового підключення до мережі Internet та відповідає оптимальним масогабаритним показникам. Функції блоку: керувати пристроями та обробляти дані з датчиків, а також контроль обміну даними з Telegram ботом .

Запропонована система «розумного будинку» дозволяє керувати будь-яким побутовим приладом. Різноманіття датчиків, які можуть бути підключені, залежить від універсальності програмного забезпечення, а саме – функціоналу Telegram бота та блоку обробки та керування.

Дані рішення дозволять створити універсальну, недорогу систему «розумного» будинку, яка буде використовувати сучасні технології для її керування та програмування.

Література

1. Огляд систем «розумного будинку» на ринку України : URL: <https://nachasi.com/2018/06/25/smart-house-faq/> (дата звернення: 18.03.2020).
2. What is Telegram ? : URL: <https://telegram.org/faq#q-what-is-telegram-what-do-i-do-here> (дата звернення 18.03.2020).
3. Відомості про Telegram ботів : URL: <https://tlgrm.ru/docs/bots> (дата звернення 19.03.2020).
4. Специфікація мікрокомп'ютера Nano Pi NEO 2 : URL: http://wiki.friendlyarm.com/wiki/index.php/NanoPi_NEO2 (дата звернення 19.03.2020).

FUTURE 6G NETWORK FUNCTIONALITY AND PERFORMANCE**Kremenetskaya Y.A., Makarenko A.O., Hetmanets O.V., Trintina N.A.***State University of Telecommunications of the**Ministry of Education and Science of Ukraine**E-mail: ya.cremen@ukr.net, makarenkoa@ukr.net,**agetman@ukr.net, trintina2015@gmail.com***Функциональные возможности и производительность будущих сетей 6G**

В данной статье мы анализируем скорости передачи информации, новые приложения, особенности реализации телекоммуникационных систем в терагерцовом диапазоне частот. Особенностью работы в терагерцовом диапазоне основывается на свойствах материалов, связанных с проблемами зависимости пропускной способности от потребляемой мощности. Показано, что терагерцевые частоты, вероятно, будет первым беспроводным спектром, который может обеспечить расчеты в режиме реального времени.

While 5G is being developed for the spectrum in the millimeter wave range (MMR) and promises data rates of up to 100 Gb/s, future 6G networks will operate in frequency bands from 100 GHz to 1 THz, where higher data rates are possible. Short wavelengths in the MMR and the terahertz (THz) band will allow massive spatial multiplexing when transmitting data through a hub, as well as incredibly accurate sounding, visualization, spectroscopy and other functions.

The THz range, which is described as the range from 100 GHz to 3 THz, can provide secure communication over highly sensitive communication lines, for example, in the sphere of information security, due to the fact that extremely short wavelengths (of the order of microns) allow the use of antennas with extremely high amplification and small dimensions. There is very high atmospheric attenuation at frequencies of the THz range (Fig. 1). Here, highly directional “pencil” beam antennas (phased array antennas) are used to transmit the signal, to compensate the increase in losses, which increase in proportion to the square of the carrier frequency for a fixed antenna aperture size. Although narrowly directed signal emission does not guarantee complete protection against listening, this feature makes THz signals extremely difficult to intercept.

A theory called consumption factor theory (CF with a metric measured in bit/s/W) provides tools for quantitative analysis and development of approaches for understanding the power tradeoff in any communication system, especially when the frequency rises above 100 GHz.

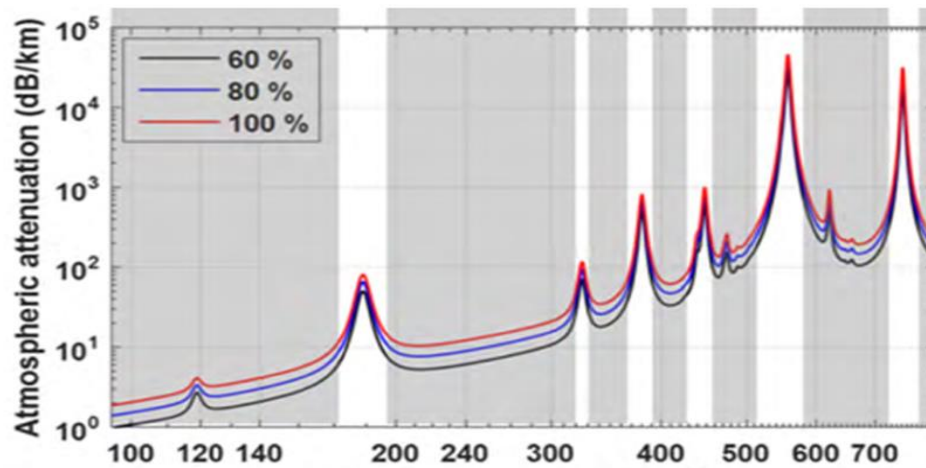


Fig. 1. Absorption in the atmosphere of electromagnetic waves at sea level as a function of frequency under different humidity conditions.

It was justified by the theory of the factor that energy consumption at high frequencies has the greatest impact on CF. The power increases with increasing bandwidth, while for a very simple radio transmitter, the required power for the auxiliary processor of the main frequency band and generator is small compared to the supplied radiated power, energy efficiency does not depend on the bandwidth. CF theory proves that for antennas with a fixed physical aperture it is more energy efficient to switch to the MMR and THz ranges. They provide a significantly wider bandwidth and increase energy efficiency in bits per second per watt (bps/W) compared to existing communications networks operating at frequencies less than 6 GHz.

The European Telecommunications Standards Institute (ETSI) and the International Telecommunication Union (ITU) are currently developing recommendations for allocating frequency bands above 95 GHz. In March 2019, the Federal Communications Commission (FCC) voted to open the spectrum above 95 GHz for the first time in the United States. The FCC provided 21.2 GHz spectrum for unlicensed use and authorized experimental licensing up to 3 THz. A group of innovative companies and universities, united to eliminate regulatory barriers for technologies, which use frequencies in the range from 95 GHz to 275 GHz in the USA, made recommendations to the FCC and the National Committee. The Telecommunications and Information Administration (NTIA) has called for promoting increased access to the spectrum above 95 GHz for non-federal use in January 2019. In 2017, the Institute of Electrical and Electronics Engineers formed the IEEE 802.15.3d task force for the global use of Wi-Fi at frequencies from 252 GHz to 325 GHz. The world's first wireless standard was created for 250-350 GHz, with a nominal PHY data rate of 100 Gbit/s and a channel bandwidth from 2 GHz to 70 GHz. The ultra-high data transfer speeds provided by

wireless local area networks and cellular networks in the MMR and THz range will provide in the future: ultra-fast download speeds for computer communications, autonomous vehicles, robotic control, high-resolution holographic applications, video, conferences and high-speed wireless data switching (circuit switching) in data centers.

Terahertz frequencies are likely to be the first wireless spectrum that can provide real-time computing. So in the human brain there are about 100 billion (10^{11}) neurons, each of which can trigger (turn on) 200 times per second. Each neuron connects to 1000 others, resulting in a computational speed of 20×10^{15} operations per second. Another feature of working in the THz range is based on the properties of materials. Since certain materials and gases have vibrational absorption (for example, resonances) at certain frequencies throughout the THz range, it will be possible to detect the presence of certain elements based on frequency scanning spectroscopy. Also, most surfaces of buildings exhibit significant diffuse scattering and strong specular reflections in the THz mode. Therefore, in the THz range, it is proposed to use new sensory applications, such as miniature radars for detecting gestures and contactless smartphones, spectrometers for detecting explosives and gas detection, THz body scans, air quality tests, as well as personal health monitoring systems. These promising custom features highlight the potential for combining imaging and communications in the MMR for precise positioning in 6G systems and around it.

The use of images in the MMR and range for the reconstruction of three-dimensional environmental maps in unknown environments will combine the perception, image formation and location of objects in one function (in one place and time). As shown below, mmWave and THz signals are strongly reflected from most building materials, which allow to obtain images of hidden objects (NLOS images).

Thus, THz frequencies are likely to be the first wireless spectrum in which it is possible to implement complex innovative applications in real time.

References

1. Rappaport T.S., Xing Y., Kanhere O., Ju S., Alkhateeb A., Trichopoulos G. C, Madanayake A., Mandal S., "Wireless Communications and Applications Above 100 GHz: Opportunities and Challenges for 6G and Beyond (Invited)," IEEE ACCESS, submitted Feb. 2019.
2. Ju S., Shah S., Javed M., Li J., Palteru G., Robin J., Xing Y., Kanhere O., and Rappaport T. S., "Scattering mechanisms and modeling for terahertz wireless communications," IEEE Int. Commun. Conf. (ICC), May 2019, pp. 1-7.

**АНАЛІЗ ТЕХНОЛОГІЙ ПОБУДОВИ
ВІРТУАЛЬНИХ ЗАХИЩЕНИХ МЕРЕЖ VPN**

Корман Н.А, Могилевич Д.І.

Інститут телекомунікаційних систем, КІП ім. Ігоря Сікорського

E-mail:kormannatasha21292@gmail.com

Проаналізовано основні принципи побудови віртуальних приватних мереж, досліджено основні методи захисту інформації від несанкціонованого доступу, що можуть бути реалізовані впливом природного або штучного характеру у VPN мережах.

Analysis of technologies for building virtual secure VPN networks

The basic principles of building virtual private networks are analyzed, the basic methods of protection of information against unauthorized access are investigated, which can be realized by influence of natural or artificial nature in VPN networks.

У загальному випадку VPN (англ. VirtualPrivateNetwork – віртуальна приватна мережа) – технологія, що дозволяє забезпечити одне або кілька мережових з'єднань (логічну мережу) поверх іншої мережі (наприклад, Інтернет). Суть технології віртуальних приватних мереж полягає в тому, що при підключенні до VPN сервера за допомогою спеціального програмного забезпечення поверх загальнодоступної мережі у вже створеному з'єднанні організується зашифрований канал, що забезпечує високий рівень захисту каналу інформації від небажаного втручання. Таким чином, створюється "тунель" між персональним комп'ютером і сервером, в якому всі дані зашифровані, і провайдер не розуміє, з яким сайтом працює користувач.

З'єднання з сервером через VPN має ряд переваг:

1. Створення WAN-з'єднання дуже дороге і може бути недоцільним для окремих користувачів. Дані, що передаються між двома кінцевими точками VPN, зашифрована, таким чином, жодне несанкціоноване втручання неможливе, коли інформація передається мережею загального користування.
2. Приховування конфіденційності, маскування дійсної IP-адреси.
3. Обходження географічних обмежень.

Недоліком використання VPN є збільшення кількості інформації, що передається в мережах. Це пов'язано із застосуванням спеціальних методів для шифрування даних, що призводить до підвищення навантажень на мережу [1].

Класифікувати рішення VPN можна за призначенням:

- Intranet VPN;
- Remote Access VPN;
- Extranet VPN;

- Client / Server VPN;
- Internet VPN.

Intranet VPN дозволяє створити надійні з'єднання між внутрішніми підрозділами розподіленої компанії. Для такої мережі мають на увазі: криптографічні засоби захисту інформації, надійність роботи важливих додатків, електронної пошти, швидкість і продуктивність передачі.

Remote Access VPN дозволяє створити захищений канал між сегментом корпоративної мережі (центрального офісу або філією) і єдиними користувачами, що мають доступ до корпоративного ресурсу за допомогою персонального комп'ютера.

Extranet VPN дозволяє створити захищену від несанкціонованого доступу корпоративну мережу, що використовує Інтернет-технології для внутрішньо-корпоративних цілей.

Client / Server VPN технологія надає захист даних, що передаються між двома вузлами корпоративної мережі. Особливість полягає в тому, що VPN будується між вузлами, що перебувають, як правило, в одному сегменті мережі, наприклад, між робочою станцією і сервером.

Internet VPN технологія дозволяє створити «тунель» для передачі даних, що дозволить зберегти цілісність та автентичність інформації.[2].

Фундаментом VPN на основі Internet є дві основні технології:

1. Технологія «Тунелю», що дозволяє створювати віртуальні канали
2. Методи забезпечення конфіденційності і цілісності інформації, що передається, а також автентифікації та авторизації користувачів які мають до неї доступ.

Розглянемо технологію тунелювання (tunneling) або інкапсуляція (encapsulation) - це спосіб передачі даних через проміжну мережу. Технологія «Тунелю» використовується не тільки для забезпечення конфіденційності внутрішнього пакета даних, але і для його цілісності.

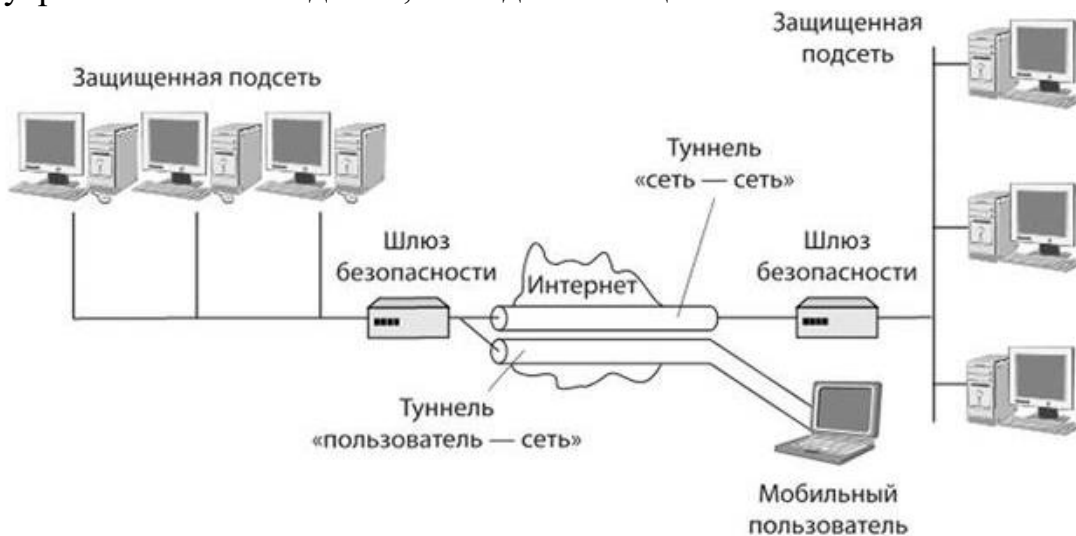


Рис. 1. Тунельна схема організації VPN-мережі.

В процесі тунелювання дані розбиваються на більш дрібні пакети, які потім будуть переміщатися по "тунелю" для транспортування до кінцевого пункту призначення. Перш ніж потрапити в Internet-тунель дані шифруються, що забезпечує їх додатковий захист та надійність. [3]

Протоколи тунелювання VPN пропонують різні функції і рівні безпеки, і кожен з них має переваги і недоліки.

Розглянемо найпоширеніші протоколи тунелювання VPN: протокол тунелювання захищених сокетів (*SSTP*), протокол тунелювання «точка-точка» (*PPTP*), протокол тунелювання другого рівня (*L2TP*), *OpenVPN* і *Internet Key Exchange* версії 2 (*IKEv2*).

SSTP використовує протокол *HTTPS* для передачі трафіку через брандмауери і веб-проксі, які можуть блокувати інші протоколи. *SSTP* надає механізм для перенесення трафіку протоколу «точка-точка» (*PPP*) по каналу *SSL*. Використання *PPP* дозволяє підтримувати надійні методи аутентифікації, а *SSL* забезпечує безпеку на рівні транспорту з розширеним узгодженням ключів, перевіркою шифрування і цілісності.

OpenVPN - програмний додаток з відкритим вихідним кодом, яке реалізує методи VPN для створення безпечних з'єднань «точка-точка» або «сайт-сайт» в маршрутизованих або мостових конфігураціях і засобах віддаленого доступу. Він використовує власний протокол безпеки, який використовує *SSL / TLS* для обміну ключами.

IKEv2 – протокол тунелювання (протокол обміну ключами, версія 2), розроблений *Cisco* і *Microsoft*, він вбудований в *Windows 7* і наступні версії. Протокол допускає модифікації з відкритим вихідним кодом, зокрема для *Linux* та інших платформ, також підтримуються пристрої *Blackberry*. *IKEv2* особливо корисний при автоматичному відновленні VPN-з'єднання, коли користувачі тимчасово втрачають свої інтернет-з'єднання.

PPTP дозволяє шифрувати мультипротокольний трафік і потім обернути його в заголовок, який буде відправлений через мережу з використанням *IP*. *PPTP* можна використовувати для віддаленого доступу і VPN-з'єднань «точка-точка». При використанні *Internet PPTP*-сервер є VPN-сервером з підтримкою *PPTP* з одним інтерфейсом в *Internet* і другим інтерфейсом в корпоративній інтрамережі. *PPTP* використовує з'єднання протоколу управління передачею для управління тунелями та інкапсуляції загальної маршрутизації для перенесення кадрів *PPP* для даних, які передаються тунелем.

L2TP дозволяє зашифрувати мультипротокольний трафік, а потім використовувати будь-який носій, що підтримує доставку даних *PPP*, наприклад, *IP* або асинхронний режим передачі. *L2TP* це комбінація *PPTP* і *Layer 2 Forwarding (L2F)*. *L2TP* представляє кращі функції *PPTP* і *L2F*. На відміну від *PPTP*, *L2TP* покладається на *IP*- безпеку (*IPsec*) в транспортному

режимі для служб шифрування. комбінація L2TP і IPsec відома як L2TP / IPsec. Обидва L2TP і IPsec повинні підтримуватися як VPN-клієнт, так і VPN-сервером.

Порівняльну характеристику протоколів шифрування наведено на Табл. 1.

Табл. 1. Характеристики протоколів шифрування.

	Шифрування	Безпеки	Швидкість
OpenVPN	256-біт	Найвище шифрування	Швидкий на високих латентних з'єднання
L2TP	256-біт	Найвище шифрування	Повільний і сильно процесорний
SSTP	256-біт	Найвище шифрування	Сповільнений
IKEv2	256-біт	Найвище шифрування	Швидкий
PPTP	128-біт	Мінімальна безпека	Швидкий

Висновки. Технологія VPN дозволяє ефективно вирішувати завдання щодо забезпечення безпеки інформаційних ресурсів, підтримати цілісність та конфіденційність інформації, що передається в локальних і глобальних інформаційних середовищах. Технологія VPN забезпечує зв'язок між мережами, а також між віддаленим користувачем і корпоративними мережами за допомогою захищеного каналу (тунелю), «прокладеного» в загальнодоступній мережі Internet.

Література

1. «VPN: плюси і мінуси, які ви повинні розглянути перед його використанням» - Електронний ресурс. – Режим доступу: <https://uk.gadget-info.com/57085-vpn-pros-and-cons-you-should-consider-before-using-it>.
2. «Концепція захищених віртуальних приватних мереж»- Електронний ресурс. – Режим доступу: <https://stud.com.ua/97437>.
3. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети - анализ технологий и синтез решений. М.: ДМК Пресс, 2004.
4. «Віртуальні захищені мережі VPN та антивірусні технології»: Електронний ресурс. – Режим доступу: https://studopedia.ru/3_28437_kontseptsiya-pobudovi-virtualnih-zahishchenih-merezh-VPN.html.

ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ДІЯЛЬНОСТІ НАУКОВИХ УСТАНОВ МЕТОДОМ ОБРОБКИ РІЗНОРІДНОЇ СЛАБОСТРУКТУРОВАНОЇ ІНФОРМАЦІЇ

Глоба Л.С., Задосенко Б.О.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: lgloba@its.kpi.ua, zadoenko.bogdan@gmail.com

Evaluation of the effectiveness of the activities of the scientific institutions by the method of processing of different slow structured information

An approach to information processing is considered, which includes information processing method based on fuzzy tree-based knowledge bases, advanced fuzzy logic model and appropriate methods, approaches and algorithms that allow structuring, formation and tuning of fuzzy knowledge base, which is the main part of the model of scientific activity evaluation institutions and agencies.

Наукова діяльність є одним із найбільш впливових чинників розвитку економіки кожної країни. Об'єктивний аналіз ефективності діяльності наукових установ та значення їх діяльності з точки зору світової та вітчизняної науки, освіти, економіки, культури, підвищення якості життя людини є вкрай актуальним. Важливим є отримання та аналіз даних відкритим та прозорим способом із застосуванням об'єктивних методів отримання показників діяльності.

Метою досліджень, яким присвячена дана доповідь, є отримання об'єктивної оцінки ефективності діяльності наукових установ НАН України з урахуванням наявних умов їхнього кадрового, інформаційного, фінансового та матеріально-технічного забезпечення; стимулювання науково-дослідної та інноваційної діяльності; прийняття обґрунтованих управлінських, організаційних та фінансових рішень; наближення до європейської практики оцінювання ефективності діяльності наукових установ [1].

Державні установи такі як міністерства та відомства відносяться до складних організаційних систем. Вони мають розвинену ієрархічну структуру, що складається з багатьох підрозділів та підлеглих установ. Інформаційні технології складають основу інформаційно-аналітичної діяльності для задач оцінювання таких об'єктів, а обробка інформації є однією з найбільш складних частин процесу оцінювання. Це обумовлено великою кількістю складних інформаційних потоків, що циркулюють в таких об'єктах, високою динамікою зміни їх структури, яка обумовлена законодавчими змінами та наявністю на кожному рівні суб'єктивних факторів, необхідністю врахування при обробці як кількісної так і якісної інформації.

Обробка інформації в таких установах виконується експертами, які, базуючись на власному досвіді та за допомогою спрощених математичних методів, проводять оцінку загального стану результатів діяльності. При цьому необхідно визначити ключові моменти такої діяльності [2]:

- оцінювана інформація часто є неповною, частина даних подається в кількісному вигляді, частина – в якісному;
- змінність вимог до проведення обробки інформації і до моделі системи;
- робота з оцінки ситуації виконується людиною на всіх рівнях ієрархії об'єкту, тому навіть в однотипних підрозділах при однакових вхідних даних можуть бути отримані різні оцінки;
- внаслідок того, що обробка інформації здійснюється людиною така система втрачає оперативність;
- виходячи з кінцевих звітів, які подаються керівнику установи, важко простежити та

визначити ті параметри, які найбільше впливають на такий стан справ.

Внаслідок цього є актуальною наукова-технічна задача розробки підходу до обробки інформації в складних організаційних системах, який би включав метод обробки інформації на основі деревоподібних баз знань, який використовує змішану, а саме чітку і нечітку, схему виведення.

Інформація може мати не тільки кількісний вигляд, але і надаватись у вигляді знань [3], а саме: правил, евристик, наборів ранжованих альтернатив, семантичних оцінок кількісних параметрів та інших характеристик, які описуються за допомогою значень лінгвістичних змінних (ЛЗ) і висловлювань. Тому необхідно використовувати такі математичні методи і підходи, які включають засоби для представлення і оперування такою інформацією, а саме методи, що базуються на теорії нечітких множин та нечіткій логіці.

В даному дослідженні запропоновано розробку підходу до обробки інформації, до складу якого повинні входити методи та алгоритми, що дозволять впорядковувати бази знань (БЗ) введенням ієрархії правил, проводити настроювання БЗ у відповідності до вхідних даних, метод обробки інформації на основі деревоподібних нечітких баз знань,

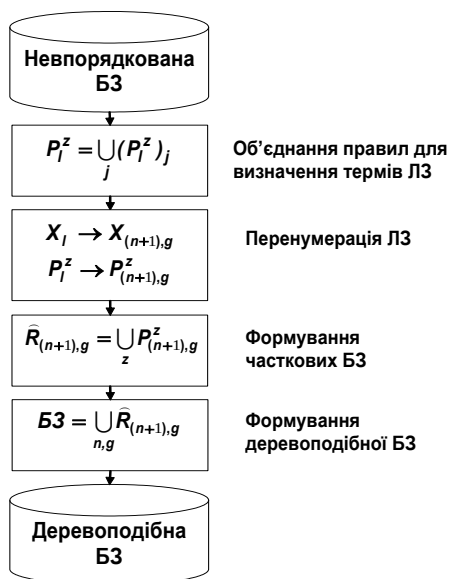


Рис.1. Кроки вирішення задачі зведення нечіткої БЗ до деревоподібної структури.

який дозволяє простежувати шлях виведення в зворотному напрямку з метою визначення всієї послідовності вершин, які вплинули на остаточне значення результуючої змінної.

Для рішення цієї задачі в роботі [4] запропоновано підхід до зведення нечіткої БЗ до деревоподібної структури за рахунок використання природної ієрархічності, а саме ієрархії оцінювання ситуації, та притаманних їм евристик. Він полягає у співставленні з кожною ЛЗ, окрім тих, що відповідають вхідним змінним, частини нечіткої БЗ, яка визначатиме залежність цієї ЛЗ від ЛЗ попереднього рівня. Таку частину нечіткої БЗ будемо називати частковою нечіткою БЗ. Тоді для кожного набору правил, що відповідають одному терму ЛЗ буде проводитись композиція, яка буде полягати в знаходженні максимуму серед всіх отриманих значень функції належності (ФН). Задля зменшення кількості перебору та усунення недоліків, що пов'язані з невпорядкованістю нечіткої БЗ,

сформулюємо задачу зведення невпорядкованої нечіткої БЗ до деревоподібної структури.

Постановка задачі: Дано:

1) $BZ = \bigcup_{l,z,j} (P_l^z)_j$ – невпорядкована нечітка БЗ, де

$(P_l^z)_j$ – j -е правило ($j = \overline{1, M}$, $M = M_{l_z}$) для визначення z -го терму ЛЗ з ідентифікатором l

2) $I = \{I_i \mid i = \overline{1, N}\}$ – множина з уведеною на ній ієрархією, що відповідає ієрархії оцінювання ситуації

3) Відповідність елементів ієрархії оцінювання ситуації лінгвістичним змінним X_i , $i = \overline{1, N}$

Отримати:

$$BZ = \bigcup_{n,g} BZ_{(n+1),g} = \bigcup_{n,g} \hat{R}_{(n+1),g} \quad (1)$$

де BZ – деревоподібна нечітка БЗ,

$$\begin{aligned}
& \text{ЯКЩО} \left(X_{n1} = X_{n1}^{k_1^{z1}} \right) \text{ТА} \left(X_{n2} = X_{n2}^{k_2^{z1}} \right) \text{ТА} \dots \text{ТА} \left(X_{nS} = X_{nS}^{k_S^{z1}} \right) \text{АБО} \\
& \left(X_{n1} = X_{n1}^{k_1^{z2}} \right) \text{ТА} \left(X_{n2} = X_{n2}^{k_2^{z2}} \right) \text{ТА} \dots \text{ТА} \left(X_{nS} = X_{nS}^{k_S^{z2}} \right) \text{АБО} \dots \\
& \hat{R}_{(n+1),g} = \text{АБО} \left(X_{n1} = X_{n1}^{k_1^{zM^z}} \right) \text{ТА} \left(X_{n2} = X_{n2}^{k_2^{zM^z}} \right) \text{ТА} \dots \text{ТА} \left(X_{nS} = X_{nS}^{k_S^{zM^z}} \right) \quad (1) \\
& \text{ТО } X_{(n+1),g} = X_{(n+1),g}^z \\
& z = \overline{1, Z_{(n+1),g}}
\end{aligned}$$

де $\hat{R}_{(n+1),g}$ – часткова нечітка БЗ для визначення залежності ЛЗ $X_{(n+1),g}$ від ЛЗ $\{X_{ns} = X_{nq_s} \mid s = \overline{1, S}\}$, n – номер рівня, q_s – номер ЛЗ на рівні n , s – номер ЛЗ у рядку-кон'юнкції, $S = S_{(n+1),g}^z$ – кількість ЛЗ у рядку-кон'юнкції, $M^z = M_{(n+1),g}^z$ – кількість рядків кон'юнкцій для визначення z -го терму ЛЗ $X_{(n+1),g}$, $X_{ns}^{k_s^{zr}}$ – терм ЛЗ X_{ns} , $k_s^{zr} = k_{ns}^{g zr}$ – номер терму.

Сформована таким чином БЗ буде мати деревоподібну структуру (рис.2). В ній можна виділити дві частини: нижню і верхню. Зауважимо, що виходячи з особливостей предметної області застосовувати автоматичні механізми формування та настроювання можливо лише для нижньої частини деревоподібної нечіткої БЗ. Це обумовлено тим, що адекватну вибірку значень вхідних та відповідних результуючих змінних можна забезпечити лише для частин нижнього рівня.

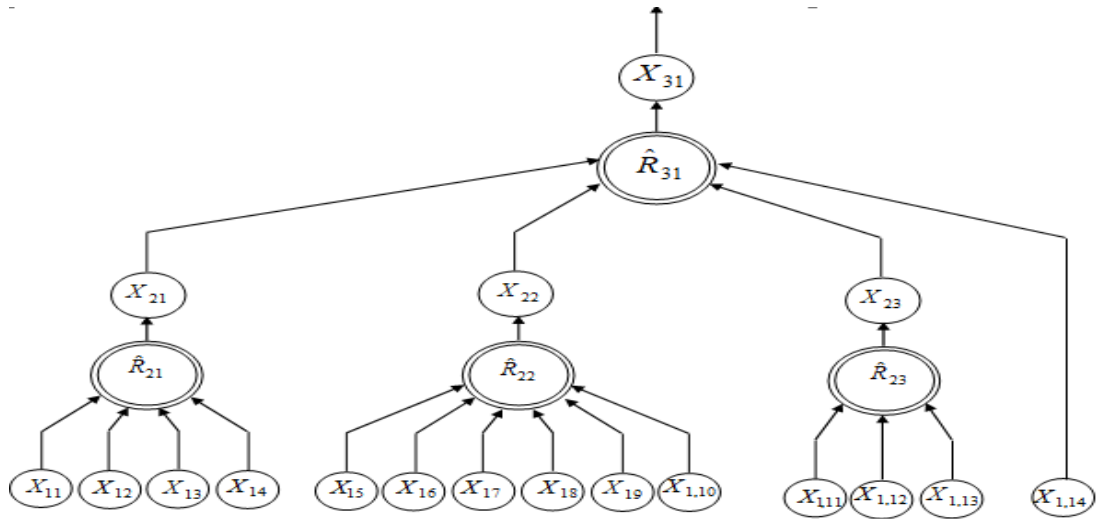


Рис. 2. Деревоподібна нечітка БЗ.

Для вирішення задач представлення знань в умовах невизначеності в працях [5,6] пропонується будувати системи нечіткого виведення на основі нечітких БЗ. Нечіткі БЗ в таких системах представляють собою сукупність лінгвістичних висловлювань типу ЯКЩО <входи>, ТО <виходи> та є частиною підсистем нечіткого виведення (ПНВ).

Рішення задач класифікації, коли результуюча змінна є якісною за своєю природою, застосовується нечітке виведення Мамдані, яке здійснюється в чотири етапи, що наведені на рис. 3:

1. Введення нечіткості.

Знаходяться ступені істинності для передумов кожного правила.

2. Нечітке виведення.

Знаходяться рівні «відсікання» для передумов кожного з правил (з використанням операції мінімум), та знаходяться «усічені» функції належності для вихідних змінних.

3. Композиція.

Проводиться об'єднання усічених функцій з використанням операції максимум, що призводить до одержання підсумкової нечіткої підмножини для змінної виходу з відповідною функцією належності.

4. Приведення до чіткості.

Додатковий етап, який використовується при необхідності перетворення нечіткої множини виведення до чіткого числа.

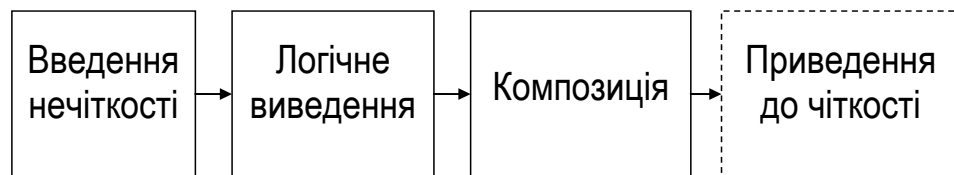


Рис. 3. Загальна схема нечіткого виведення.

Запропонований підхід у роботі [2] дозволяє проводити аналіз якості наукових досліджень у наукових установах та разом із застосуванням онтологій, які описуватимуть набори параметрів, за якими оцінюється наукова діяльність установ, дозволить розробити методику, що отримуватиме більш достовірний інтегральний узагальнюючий показник – рейтинг.

Висновки. В роботі визначено підхід до обробки інформації, який включає метод обробки інформації на основі нечітких деревоподібних баз знань, удосконалену нечітку логічну модель та відповідні способи, підходи та алгоритми, що дозволяють провести структурування, формування та настроювання нечіткої БЗ, яка є головною частиною моделі оцінки наукової діяльності установ та відомств. Також визначено підхід до зведення неупорядкованої нечіткої бази знань до деревоподібної структури, за рахунок використання ієрархічності оцінювання інформації.

Література

1. Методика оцінювання ефективності діяльності наукових установ Національної академії наук України ЗАТВЕРДЖЕНО постановою Президії НАН України від 15.03.2017 № 75 зі змінами, внесеними постановою Президії НАН України від 11.07.2018 № 241.
2. Терновой М.Ю. -ПІДХІД ДО ОБРОБКИ ІНФОРМАЦІЇ НА ОСНОВІ ДЕРЕВОПОДІБНИХ БАЗ ЗНАНЬ ЗІ ЗМІШАНОЮ СХЕМОЮ ВИВЕДЕННЯ.
3. Згуровский М.З., Доброногов А.В., Померанцева Т.Н. Исследование социальных процессов на основе методологии системного анализа. – К.: Наукова думка, 1997. – 224 с.
4. Глоба Л.С., Терновой М.Ю. Оптимизация использования базы знаний экспертной системы введением иерархии правил. // Труды седьмой международной научно-практической конференции "Современные информационные и электронные технологии" (СИЭТ-2006). – Одеса: ОНПУ. – 2006. – С.166.
5. Герасимов Б.М., Грабовский Г.Г., Рюмшин Н.А. Нечеткие множества в задачах проектирования, управления и обработки информации. –К.: Техніка, 2002. –140 с.
6. Ротштейн А.П. Интеллектуальные технологии идентификации: нечеткие множества, генетические алгоритмы, нейронные сети. – Винница: УНИВЕРСУМ, 1999. –320 с.

ЗАХИСТ ІНФОРМАЦІЇ В МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ НА ОСНОВІ REST API

Безвугляк М. С., Курдеча В. В.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: maximbezvugliak@gmail.com

Security of information on the Internet of Things based on REST API

Overview, problems of protection of information in the Internet of Things. Consideration of proposed solutions at the moment and their comparison. A modified method is proposed that improves the level of protection of information on the Internet of Things.

Огляд, проблеми захисту інформації в Інтернеті речей. Розгляд запропонованих рішень на даний момент та їх порівняння. Запропонування модифікованого методу, який покращує рівень захисту інформації в Інтернеті речей.

Інтернет речей з'єднує комп'ютерні пристрої інтегровані у повсякденні об'єкти через Інтернет, що дозволяє їм надсилати та отримувати дані. Є дві переваги, які надають комп'ютерам можливість збирати інформацію про оточення, незалежно від людини і від обробки зібраної інформації зменшуються втрати та вартість.

На сьогоднішній день запропоновані методи в захисті інформації в мережі інтернету речей мають багато недоліків в таких аспектах як:

- Інфраструктура відкритих ключів не підходить для IoT середовища, так як це стає обчислювально важким завданням обчислення шифрованого тексту через великий розмір ключа.

- Після того, як система потрапить під загрозу, її буде важко оновити. Крім того, потенційно відключення скомпрометовані системи, перевстановлюють або перезапускають програмне забезпечення або заміняють компоненти або підсистема не підходить для всіх систем ІОТ.

Усі пристрої пов'язані в одну систему повинні мати довірчу відносини одне до одного. Програмне забезпечення IoT має керувати довірчими відносинами пристроїв, щоб ці пристрої могли бути аутентифіковані та авторизовані для обміну даними. Для цього потрібно застосувати автентифікацію для комунікації з будь-яким пристроєм, що може підтвердити походження даних.

В даній роботі розглянуто захист інформації в мережі інтернету речей використовуючи REST API для безпечного з'єднання між пристроями в мережі та використання Еліптично Кривої Криптографії для безпечної авторизації пристроїв.

REST API дозволяють відкрити підключений пристрій користувачам у програмі безпечним способом.

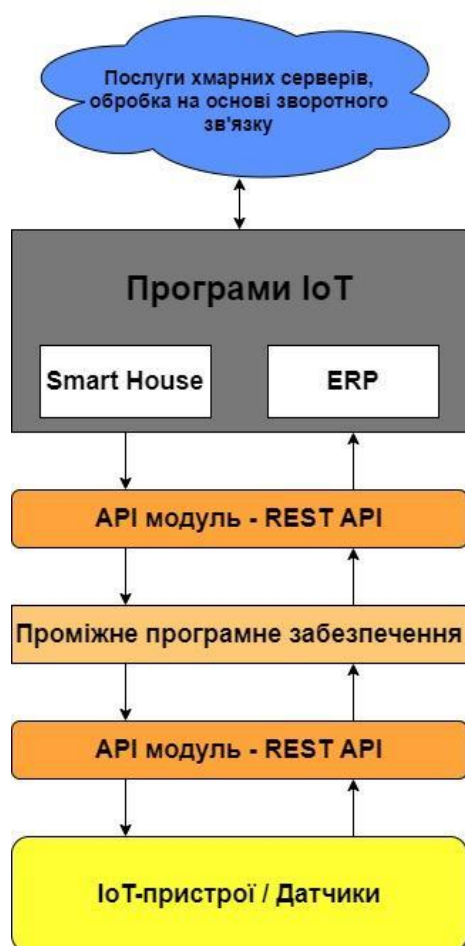


Рис. 1. Модель архітектури Проміжного програмного забезпечення в мережі інтернету речей.

RESTful API широко використовуються в сучасній мережі. Передача даних зазвичай здійснюється за допомогою JSON або XML через HTTP. Це гарна модель для неоднорідних систем. REST API робить інформацію про пристрій легкодоступною. Вони можуть стандартизувати спосіб створення, читання, оновлення та видалення даних. Усі ці операції включені до REST-запиту. API REST дозволяють делегувати та керувати авторизацією. API може автентифікуватись на сервері і сервер можуть автентифікувати API, щоб запобігти атакам в середині.

На рис. 1 представлена загальна картина ролі проміжного програмного забезпечення в IoT. У загальному сенсі маємо чотири категорії основних компонентів системи IoT - датчики, локальна мережа, яка може включати шлюз, проміжне програмне забезпечення, хмарне сховище.

Доступно багато протоколів авторизації. Наприклад, OAuth - це відкритий протокол авторизації, який може надати доступ до ресурсу через програмне забезпечення, використовуючи ім'я користувача, пароль та токени.

Крок 1: - Для реєстрації пристрою потрібен авторизований користувач, який вже створив онлайн-акаунт через проміжне програмне забезпечення.

Крок 2: - Щоразу, коли запит на автентифікацію надходить від пристрою IoT, шлюз перевіряє запит пристроїв, включаючи корисне навантаження пристрою, отримуючи доступ до відкритого REST API. Далі шлюз, у свою чергу, робить запит на доступ до відкритого API з власними обліковими даними. Запит буде містити ідентифікатор шлюзу та секретний ключ як вхідні параметри. API буде ідентифікувати та авторизувати шлюз, і підтверджувати запит. Усі методи в API REST вимагають автентифікації. Після того, як шлюз буде авторизований, відповідь у зашифрованій формі, що містить деталі пристрою, надсилається назад до шлюзу. Тепер після перевірки шлюз надає маркер доступу до пристрою, і пристрій може надсилати дані в реальному часі на шлюз. Безпечні рішення реалізуються таким чином, щоб виявити небажані вторгнення та запобігати зловмисним атакам на комунікаційному шарі. Крім забезпечення від атак типу атак Replay, відсутній ідентифікатор відгадування атак, заборонений вхід, анонімність користувача та анонімність датчика вузла. На рис. 2 наведено

огляд вимоги безпеки для різних ступенів системи IoT.

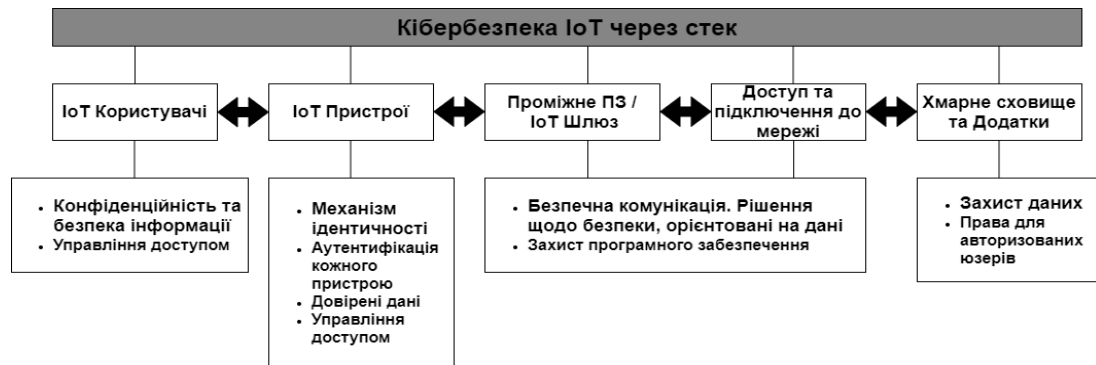


Рис. 2. Модель захисту для системи інтернету речей.

Запропоновані особливості застосування REST API дозволяють підвищити безпеку інформаційного обміну IoT :

- Пристрої IoT ізольовані і не мають взаємодії із зовнішнім світом. Вони підключені до шлюзу і цей шлюз діє як інтерфейс до Інтернету для пристроїв IoT. Тому що розумні пристрої шлюзу можуть бути захищені в підприємстві за декількома брандмауерами і не потребуватимуть вхідних даних порта.
- Зв'язок між шлюзом IoT та проміжним програмним забезпеченням захищене традиційними криптографічними алгоритмами. Не потрібно використовувати легковисні алгоритми, оскільки дві сторони не є ресурсообмеженими.
- Про автентифікацію та авторизацію піклується REST API, що робить весь процес менш складним та сумісним з індустріальними стандартами.

В даній роботі розглянуто архітектуру проміжного програмного забезпечення, яка забезпечує рішення безпеки для учасників, і сформовано особливості застосування REST API для шифрування даних. У запропонованому рішенні проміжного програмного забезпечення всі обмеження системи IoT приймаються до розгляду. REST API використовується для зв'язку та обміну даними. Проміжне програмне забезпечення успішно допомагає IoT в розробці шляхом викриття API REST та надання інтерфейсу для користувача, щоб зареєструвати пристрої в мережі IoT, а потім надання безпечного доступу до даних, зібраних пристроєм. Такий підхід має підвищити безпеку IoT мережі.

Література

1. Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80-84.
2. "REST API for Oracle Internet of Things Cloud Service", docs.oracle.com/en/cloud/paas/iot-cloud/iotrq/QuickStart.html.
3. Wu, F., Xu, L., Kumari, S., & Li, X. (2017). "A privacy-preserving and provable user authentication scheme for wireless sensor networks.
4. Ayoade, G., El-Ghamry, A., Karande, V., Khan, L., Alrahmawy, M., & Rashad, M. Z. (2018). Secure data processing for IoT middleware systems. The Journal of Supercomputing, 1-26.

МОДЕЛІ ІДЕНТИФІКАЦІЇ ТА АУТЕНТИФІКАЦІЇ В СИСТЕМАХ ХМАРНИХ ОБЧИСЛЕНЬ ДЛЯ ВЕБ-СЕРВЕРІВ ТА МОБІЛЬНИХ ДОДАТКІВ З ІНТЕЛЕКТУАЛЬНОЮ ПІДТРИМКОЮ ВИБОРУ

Пилипчук А. О.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: pylypchukangelina@gmail.com

Models of identification and authentication in cloud computing systems for web servers and mobile applications with intelligent support of choice

Six variants of mathematical models of authentication during users work with mobile applications in cloud area are represented. The intelligence approach for choice of identification and authentication system on the base of expert system knowledge base roles is proposed.

Моделі та засоби ідентифікації та аутентифікації користувачів в системах хмарних обчислень є важливим та актуальним напрямком дослідження та розробок в області захисту інформації. Ідентифікація (Identification) – процедура розпізнавання користувачів по їх ідентифікатору. Аутентифікація (Authentication) – процедура перевірки справжності заявленого користувача, процесу чи пристрою [1].

В даній доповіді розглядається інтелектуальний підхід для вибору варіантів системи ідентифікації та аутентифікації (СІА). Даний підхід базується на основі складання бази правил вибору, в якості інтелектуального інструменту застосовуються засновані на правилах експертні системи (ЕС). ЕС в базі знань включає опис класифікаційних правил СІА, відповідних профілям легальних користувачів. Експерт формує базу правил для вибору варіанта СІА. Робота такої ЕС може базуватись як на експертному підході, так і в автоматичному режимі сервера. Для першого варіанту організовується діалог, в ході якого виявляються побажання чи вимоги користувача чи адміністратора. На основі результатів опитування формується варіант. В автоматичному режимі серверу варіант СІА формується по профілям легальних користувачів.

Для реалізації даного підходу розглянемо моделі аутентифікації та ідентифікації користувачів при роботі з мобільними додатками в хмарному середовищі. Представлено шість математичних моделей аутентифікації:

Аутентифікація по паролю з сервером додатків. Ця модель заснована на тому, що користувач повинен представити серверу додатків username – U_n та password – P_s для успішної ідентифікації та аутентифікації в системі. Нехай, X – користувач, B – браузер, S – сервер додатків, A – ознака аутентифікована, n – унікальне значення, H – хеш функція, C – процес шифрування, P – k -ий додаток. Базова модель аутентифікації матиме вигляд:

$$X(U_n, P_s) \rightarrow B \rightarrow S_p; S_p(A) \rightarrow B \rightarrow X.$$

Аутентифікація з додатками. У цій моделі користувач повинен представити додатку username – U та password – P для успішної ідентифікації та аутентифікації в системі. Має наступний вигляд:

$$X(U_n, P_p) \rightarrow B \rightarrow P_k(S_p); P_k(S_p(A)) \rightarrow B \rightarrow X.$$

Аутентифікація по сертифікату. Нехай, CA – сервер аутентифікації, $C_a(k)$ – сертифікат користувача, K_s – секретний ключ. Вигляд моделі:

$$X(C_a(k), K_s) \rightarrow CA; CA(C_a(k), CA) \rightarrow X;$$

$$X(C_a(k), CA) \rightarrow S_p; S_p \rightarrow CA; S_p(A) \rightarrow B \rightarrow X.$$

Модель більш надійна, однак є важкості з поширенням та реалізацією.

Аутентифікація по одноразовим паролем. Зазвичай використовується додатково до аутентифікації по паролем для реалізації двох-факторної аутентифікації (2FA). Для цього користувачу потрібно представити дані двох типів для входу в систему: щось, що він знає (наприклад, пароль), та щось, що він має (наприклад картку). Реалізація даної моделі можлива завдяки токенам, які можуть генерувати одноразові паролі на основі секретного ключа, введено в них, поточного часу – $T(K_s, t)$ та запиту одноразового паролю – R . Модель представлена в наступному вигляді:

$$X(U_n, P_s) \rightarrow B \rightarrow P_k(S_p); P_k(S_p, R) \rightarrow X;$$

$$X(T(K_s, t))) \rightarrow B \rightarrow P_k(S_p).$$

Аутентифікація по ключам доступу. Ця модель використовується для аутентифікації пристроїв, сервісів чи інших додатків при зверненні до веб-сервісів WS , що зберігаються на хмарному сервері – S_{ws} , засобом аутентифікації є ключ доступу – K_a . Модель має вигляд:

$$X(U_n, P_s) \rightarrow B \rightarrow S_{ws}; S_{ws}(K_a) \rightarrow X; X(K_a) \rightarrow P_k(S_{ws}).$$

Аутентифікація по токенам. Дана модель аутентифікації застосовується при побудові розподілених систем Single Sing-On (SSO), де один додаток – SP (service provider) делегує функцію аутентифікації користувачів другому додатку IP (identity provider). Наприклад, вхід в додаток через обліковий запис в соціальних мережах. Токен $T(P_i)$ генерується $IP(P_i)$, де P_i – параметр токена. Модель має вигляд:

$$X(K_a) \rightarrow B \rightarrow IP; IP(n) \rightarrow B \rightarrow X;$$

$$X(H(n, K_s) \rightarrow B \rightarrow IP(T(P_i)) \rightarrow X; X(T(P_i)) \rightarrow SP.$$

Моделі ідентифікації базуються на трирівневому семифакторному підході класифікації ідентифікаторів [3]: (1) як характеристики приналежності – універсальний (U), корпоративний (C), особистий (P); (2) для розпізнання особистості власника – анонімний (N), персональний (I); (3) доступ власника до ресурсів – одноразовий (O) та багаторазовий (M). Отже в електронному просторі маємо різновид ідентифікацій представленої сімки: $MCI = (UNM, UPO, UPM, CNO, CNM, CPM, IPM)$, де використані наступні ідентифікатори: UNM - універсальний анонімний багаторазовий (користувач

інтернету), UPO - універсальний персональний одноразовий (генератор одноразових паролей), UPM - універсальний персональний, що міститься в реєстрі (електронний паспорт), CNO - корпоративний анонімний одноразовий (банківська карта), CNM - корпоративний анонімний багаторазовий, CPM - корпоративний персональний багаторазовий (пропуск - смарт-карта), IPM - особистий персональний багаторазовий (біометрія на карті чи сервері). Виникає завдання вибору моделі аутентифікації та моделі ідентифікації з інтелектуальною підтримкою [2].

Розглянемо підхід для підтримки прийняття рішень по вибору моделей аутентифікації та моделей ідентифікації. Пропонується класифікація системи аутентифікації по ознакам виконання цілей та завдань [3]. Процес аутентифікації складається з послідовно виконуючих процедур двох класів: до першого відносяться процедури реєстрації нового користувача та зберігання інформації аутентифікації, до другого - процедури представлення інформації аутентифікації, протоколи обміну, валідація та прийняття рішення про результат проходження перевіркою стороною процесу аутентифікації. Модель класифікації аутентифікації - *MCA* – представимо трійкою :

$$MCA = \{A, W, C\},$$

де *A* - доступність (accessibility), *T* - цілісність (wholeness), *C* - конфіденційність (confidelity). Деталізації цілей та завдань виразимо таким чином:

$A = \{GA, DA, CA, PA\}$; $W = \{WS, WRR, WAP, WPC\}$; $C = \{CPP, CAP, CPC\}$, де *GA* - гарантія обробки запитів користувачів на аутентифікацію, *DA* - поділ доступу користувачів, *CA* - контроль доступу, *PA* - персоніфікація доступу; *WS* - цілісність ПО, *WRR* - цілісність облікових записів, *WAP* - цілісність аутентифікаційної інформації користувачів; *WSC* - цілісність аутентифікаційної інформації користувачів в хмарному середовищі; *CPP* - конфіденційність облікових записів, *CAP* - конфіденційність аутентифікаційної інформації користувачів, *CPC* - конфіденційність аутентифікаційної інформації користувачів в хмарному середовищі.

Висновок. Експертна система методом складання бази правил вибору допоможе підібрати найбільш безпечніший варіант системи ідентифікації та аутентифікації для мобільних додатків.

Література

1. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам / А.А. Афанасьев, М.: Горячая линия - Телеком, 2012. 550 с.
2. Вишняков В.А. Информационная безопасность в корпоративных системах, электронной коммерции и облачных вычислениях: методы, модели, программно-аппаратные решения / В.А. Вишняков, Минск: Бестпринт, 2016. - 276 с.
3. Сабанов А.Г. Принципы классификации систем идентификации и аутентификации по признакам соответствия требованиям информационной безопасности // Электросвязь, 2014, № 2. С. 6-9.

УДОСКОНАЛЕНА АРХІТЕКТУРА МЕРЕЖІ ДЛЯ ХМАРНОГО ІНТЕРНЕТУ РЕЧЕЙ

Пороло Є.О., Курдеча В.В.

Інститут телекомунікаційних систем КПП ім. Ігоря Сікорського, Україна

E-mail: jeykeuwork@gmail.com

Improved architecture of the cloud-IoT network

This article proposes the use of Data Bank technology in cloud-based IoT architecture. This structure aims to protect the personal data of users, allowing them to control what type of data is being transmitted and provides supportive tools for transaction visualization and privacy compromise.

В даній статті запропоновано застосування технології Data Bank в хмарній архітектурі IoT мережі. Дана структура спрямована на захист персональних даних користувачів, дозволяючи їм контролювати який тип даних передається та надає допоміжні інструменти для візуалізації транзакцій та компрометації конфіденційності.

На даний час отримав розвитку спосіб надання безкоштовних послуг в обмін на дані користувачів. Технології Інтернету речей приносять багато переваг користувачам, але також викликають занепокоєння щодо безпеки та конфіденційності. Більшість пристроїв можуть передавати особисті дані третім особам. Внаслідок цього, існує явна потреба в розробці хмарної інфраструктури Інтернету речей, щоб дозволити користувачам контролювати свої дані. Для цього пропонується хмарна архітектура Інтернету речей, названу Data Bank, яка дозволяє користувачам налаштовувати збір даних і політики контролю доступу.

Концепція Data Bank пропонується в якості настанови для постачальників послуг. Запропонована структура спрямована на управління даними, що виходять з пристроїв Інтернету речей, шляхом надання політики збору даних на рівні пристроїв і політики обміну даними на хмарному рівні.

Основні особливості цієї архітектури

- сховище(repository);
- механізм конфіденційність-корисність;
- забезпечення контролю доступу.

«Сховище» даних дозволяє користувачам зберігати свої особисті дані в безпеці. Дані тимчасово зберігаються в Data Pocket перед перенесенням в «Сховище» даних в хмарі. Data Pocket (який є локальним і знаходиться під контролем користувача) зберігає встановлену політику конфіденційності і фільтрує дані користувачів перед завантаженням до хмарного сховища. Механізм «конфіденційність-корисність» спрямований на пошук правильного балансу між отриманими перевагами та втратою конфіденційності і пропонує послуги користувачам на основі заздалегідь визначених критеріїв конфіденційності користувачів. «Забезпечення контролю доступу» обмежує постачальників послуг в доступі до даних користувачів. Постачальники послуг надають послуги користувачеві

безкоштовно в обмін на особисті дані та / або збір даних про використання сервісів від користувачів. Data Bank обмежуватиме доступ до даних на основі політики контролю доступу. Запропоновано модифікувати архітектуру Інтернету речей за рахунок зміни специфіки застосування технології Data Bank - пропонується 4-х рівнева архітектура збереження конфіденційності в процесі збору та обміну даними для хмарних платформ Інтернету речей (рис.1).

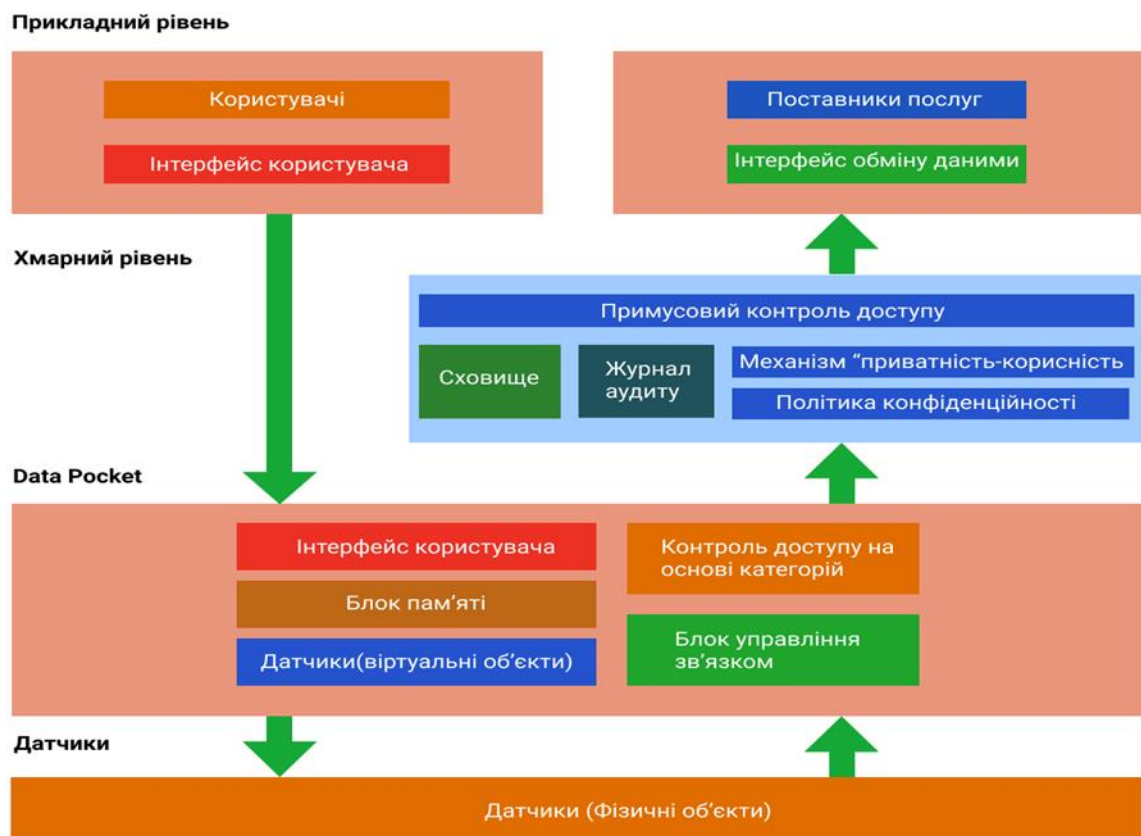


Рис. 1. Модифікована архітектура IoT з використанням Data Bank

Прикладний Шар - це верхній шар, який має справу з користувачами, службами, інтерфейсом користувача та інтерфейсом обміну даними/менеджером компонентів. Інтерфейс визначає: як користувачі повинні взаємодіяти з Data Bank.

Хмарний шар - цей шар містить п'ять основних компонентів, включаючи модуль забезпечення контролю доступу, сховище(геро), журнал аудиту, механізм конфіденційність-корисність і політику конфіденційності.

Data Pocket Layer - цей шар містить інтерфейс користувача, блок пам'яті, датчики, модуль примусового збору даних на рівні пристрою і блок управління зв'язком. Метою даного інтерфейсу є захоплення улюблених користувачів.

Шар датчиків (фізичні об'єкти) - цей шар містить пристрої Інтернету речей, підключені через Інтернет або локальну мережу. Зв'язок між об'єктами в цьому шарі заборонено. Це дозволено тільки через віртуальні об'єкти, які керуються блоком управління зв'язку в Data Pocket.

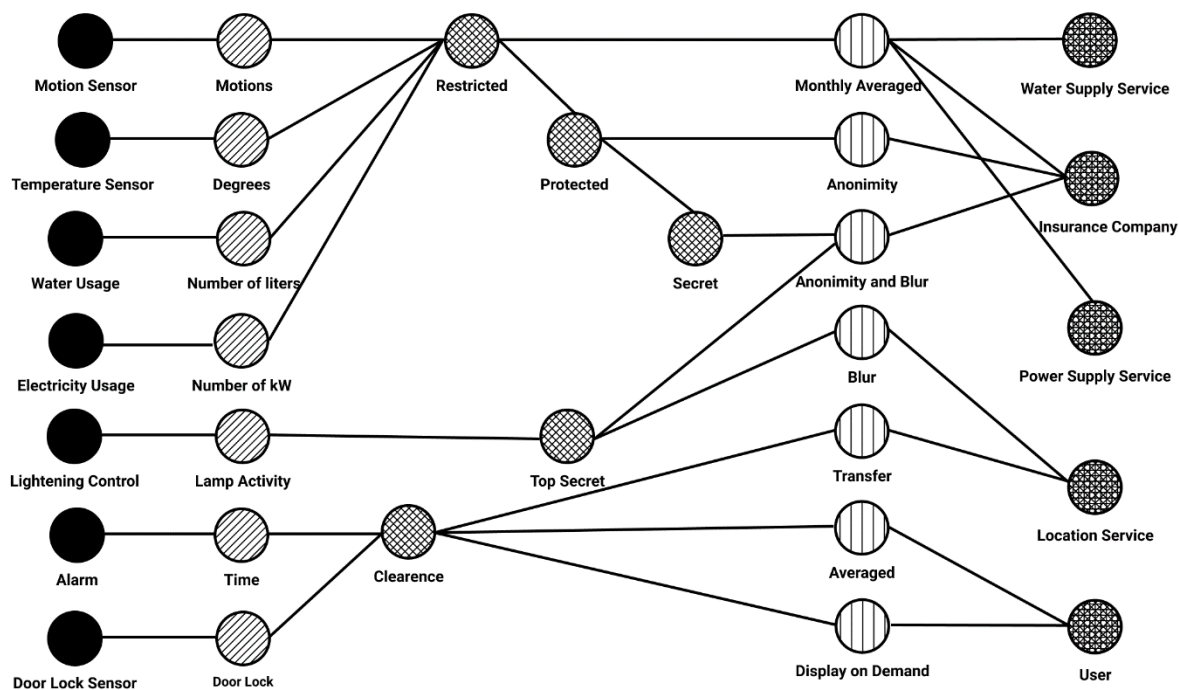


Рис. 2. Приклад політики та шляху даних в системі розумний дім.

Розроблено прототип розумного дому (рис.2), для показу концепції Data Bank.

Існує декілька подібних підходів, що вирішують питання конфіденційності, два з яких близькі до даного: [1] DataBox та [3] Personal Data Vault. Концепцію запропоновану в цій статті можна розглядати як уточнення ідеї Data Vault шляхом додавання елемента управління на рівні збору даних так, що користувачі можуть вибирати, які дані зберігаються в сховищі.

В даній статті було розглянуто багаторівневу архітектуру мережі для хмарного-IoT, названу Data Bank, для зберігання та керування особистими даними. Це дає користувачам детальний контроль над їхніми даними і дозволяє їм ділитися інформацією з поставниками послуг відповідно до визначеної користувачем політики. Сервіси можуть отримувати доступ до даних лише в тому випадку, якщо вони уповноважені робити це за допомогою визначеної користувачем політики обміну даними.

Література

1. H. Haddadi, H. Howard, A. Chaudhry, J. Crowcroft, A. Madhavapeddy, and R. Mortier. Personal Data: Thinking Inside the Box. ArXiv e-prints, January 2015.
2. "Access control models for virtual object communication in cloud-enabled IoT," in IEEE International Conference on Information Reuse and Integration (IRI), 2017, pp. 16–25.
3. Min Mun, Shuai Hao, Nilesh Mishra, Katie Shilton, Jeff Burke, Deborah Estrin, Mark Hansen, and Ramesh Govindan. Personal data vaults: A locus of control for personal data streams. In Proceedings of the 6th International Conference, Co-NEXT '10, pages 17:1–17:12, New York, NY, USA, 2010. ACM.
4. S. Barker, "The next 700 access control models or a unifying meta-model?" in Proceedings of the 14th ACM Symposium on Access Control Models and Technologies, ser. SACMAT '09. New York, NY, USA: ACM, 2009, pp. 187–196.

АНАЛІЗ МЕТОДІВ СЕРІАЛІЗАЦІЇ ОБ'ЄКТІВ ДЛЯ ПОБУДОВИ ПЛАТФОРМИ ВЕЛИКИХ ІНДУСТРІАЛЬНИХ ДАНИХ

Попенко Д.В., Курдеча В.В.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: demyd.popenko@gmail.com

Analysis of object serialization methods for building a platform of big industrial data

The article describes existing methods of object serialization, investigates and analyzes the performance of methods for different amounts of computational objects, which is important for building a platform for collecting big industrial data. A method has been identified that will most effectively convert data structures into a bit sequence.

У статті описуються існуючі методи серіалізації об'єктів, досліджено і проаналізовано продуктивність методів при різній кількості обчислювальних об'єктів, що є важливим для побудови платформи великих індустріальних даних. Визначено метод, який дозволить за критерієм часу найбільш ефективно перетворювати структури даних у послідовність бітів.

Індустріальний Інтернет речей - це система об'єднаних комп'ютерних мереж і промислових об'єктів, які пов'язані між собою вбудованими датчиками і програмним забезпеченням для збору, обробки та обміну даними. Це забезпечує проведення віддаленого моніторингу та управління в автоматичному режимі без втручання людини.

Метою даної роботи є вибір методу серіалізації, який забезпечить мінімальні часові витрати на обробку об'єктів.

Отримана з пристроїв на підприємстві інформація може бути використана для запобігання позапланових простоїв, поломок устаткування, скорочення позапланового техобслуговування і збоїв в управлінні поставками, тим самим дозволяючи підприємству функціонувати більш ефективно. Але різні види пристроїв мають різні типи даних, які в сукупності являють собою масивні неоднорідні набори інформації з багатьох джерел. Це призводить до великих витрат на збір даних та інтеграцію обладнання з системою обробки даних. Саме тому необхідно вибрати найбільш продуктивний метод серіалізації, який забезпечить мінімальний час перетворення будь-яких структур даних в бітову послідовність і передачу об'єктів по мережі.

На рисунку 2 наведено загальний принцип процесу серіалізації.



Рис.2. Загальний процес серіалізації.

Розглянемо чотири методи: Protobuf, Kryo, Protostuff, Jackson.

Jackson [2] орієнтований на поєднання швидкості та ергономічності. Він пропонує три варіанти обробки JSON. Модель дерева забезпечує оптимізовані для обробки дані, представлені у вигляді дерева JSON документа.

Protostuff [3] – це розширена версія протокольних буферів (Protocol Buffers) від Google. Protostuff підтримує багато форматів, серед яких JSON, XML, YAML та KVP.

Протокол буферів (Protocol Buffers) [4] використовується в Google для кодування структурованих даних в ефективному форматі. Він кодується до двійкових даних для забезпечення меншої та швидшої серіалізації.

Kryo [5] - це середовище серіалізації Java, орієнтоване на швидкість, ефективність та зручність API. Фреймворк надає клас Kryo в якості основної точки входу до всіх його функціональних можливостей.

Для оцінювання часу серіалізації, використовуючи дані дослідження [6] необхідно визначити функції, якими можна описати час серіалізації та десеріалізації в залежності від кількості оброблюваних об'єктів. Для цього необхідно заздалегідь підготувати набори інформації, які ми будемо подавати як вхідні дані для чотирьох методів серіалізації. Для фіксації часу і отримання точніших результатів проведемо три ітерації для різної кількості об'єктів. У таблиці 1 наведені результати для кожного методу.

Таблиця 1. Час серіалізації та десеріалізації для різних методів.

Кількість об'єктів серіалізації	1*10 ⁴	1*10 ⁵	1*10 ⁶	1*10 ⁷	1*10 ⁸
Kryo (сек)	0.3	0.44	2.33	18.42	215
Protostuff (сек)	0.11	0.24	1.11	8.37	87
Protobuf (сек)	0.45	0.62	1.2	8.73	82
Jackson (сек)	1.7	1.89	3.58	18.67	246

Використовуючи метод лінійної інтерполяції [7] отримали систему рівнянь для кожного методу. Для прикладу нижче наведено формулу, яка описує час серіалізації для методу Kryo.

$$t = \begin{cases} 0.3 + 1.556 * 10^{-6} * (n - 10^4), & 0 \leq n \leq 10^5 \\ 0.44 + 2.1 * 10^{-6} * (n - 10^5), & 10^5 < n \leq 10^6 \\ 2.33 + 1.788 * 10^{-6} * (n - 10^6), & 10^6 < n \leq 10^7 \\ 18.42 + 2.184 * 10^{-6} * (n - 10^7), & 10^7 < n \leq 10^8 \end{cases} \quad (1)$$

де t – час серіалізації та десеріалізації, n – кількість об'єктів.

Для візуалізації отриманих результатів на рисунку 3 побудовані графіки на основі отриманих рівнянь.

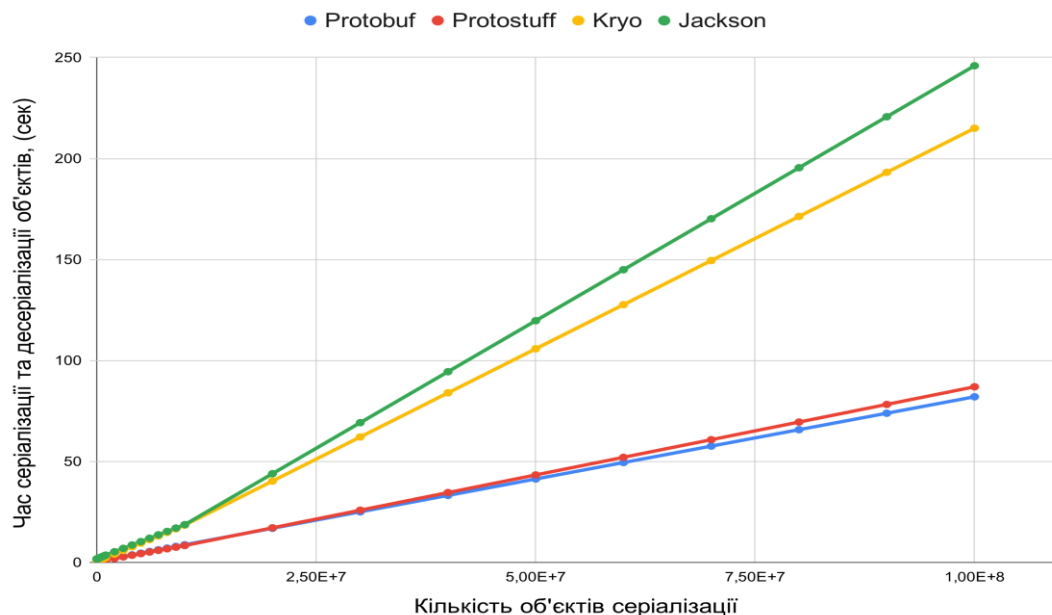


Рис.3. Час серіалізації чотирьох методів для різної кількості об'єктів обробки.

В даній роботі розглянуто та проаналізовано чотири методи серіалізації: Kryo, Protostuff, Protobuf, Jackson. Отримано системи рівнянь для кожного методу. На основі їх аналізу визначено найефективніший метод в залежності від кількості об'єктів серіалізації за критерієм часу обробки.

Найкращий результат отримано використовуючи Protobuf. В подальшій роботі при проектуванні платформи великих промислових даних отримані системи рівнянь можна використовувати для визначення часу, який витрачається на серіалізації та десеріалізації структур даних.

Література

1. State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating [Електронний ресурс] // IoT Analytics. – 2018. – Режим доступу до ресурсу: <https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/>.
2. Serialization with Jackson [Електронний ресурс] // Akka Documentation – Режим доступу до ресурсу: <https://doc.akka.io/docs/akka/current/serialization-jackson.html#serialization-with-jackson>.
3. Protostuff - java serialization library, proto compiler, code generator [Електронний ресурс] – Режим доступу до ресурсу: <https://github.com/protostuff/protostuff>.
4. Protocol Buffers - Google's data interchange format [Електронний ресурс] – Режим доступу до ресурсу: <https://github.com/protocolbuffers/protobuf>.
5. Introduction To Kryo [Електронний ресурс] // Baeldung. – 2019. – Режим доступу до ресурсу: <https://www.baeldung.com/kryo>.
6. Big Data-Based Improved Data Acquisition and Storage System for Designing Industrial Data Platform [Електронний ресурс] // IEEE. – 2019. – Режим доступу до ресурсу: <https://ieeexplore.ieee.org/document/8681030>.
7. Linear interpolation [Електронний ресурс] // Wikipedia – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Linear_interpolation.

МОДИФІКОВАНИЙ МЕТОД УПРАВЛІННЯ ІНФРАСТРУКТУРОЮ МЕРЕЖІ ПРОМИСЛОВОГО ІНТЕРНЕТУ РЕЧЕЙ

Давидюк А.М., Курдеча В.В.

Інститут телекомунікаційних систем

КПІ ім. Ігоря Сікорського, Україна

E-mail: mr.wokawoka@gmail.com

Modified network infrastructure management method for industrial internet of things

Today there is a problem with automation and work simplification for data warehouses. This problem is also acute for the industrial Internet of Things networks, as these networks operate on a large amount of data. Our solution offers the creation of a cluster with non-relational databases and containerization of the databases themselves as a fast, cheap and reliable way to deploy the environment

Причина виникнення проблеми

На сьогоднішній день постає проблема з автоматизацією і спрощенням роботи з сховищами даних. Ця проблема також гостро постає для мереж промислового Інтернету речей, оскільки ці мережі оперують великою кількістю даних.

Результати показують, що кластеризація компонентів бази даних зменшить час обробки даних та забезпечить більшу цілісність даних. А контейнеризація допомагає спростити адміністрування та оптимізувати ресурси.

З розвиненим технологічним рівнем та відповідною доступністю обчислювальних пристроїв зменшується ризик відмови систем системи, а також збільшується надійність збереження даних.

Загалом, кластеризація в архітектурі сервера може бути універсальним варіантом розповсюдження, а також збереження цільових даних у разі відмови. Таким чином отримавши широкі доповнення до сучасних систем. На всіх рівнях трирівневої структури IoT. Контейнеризація ж дозволить зменшити кількість виділених ресурсів для кожного вузла кластеру, а налаштування алгоритму шаблонного розгорнення контейнерів дозволить зробити адміністрування та управління мережею автономними та зручними у налаштуваннях.

То ж наше рішення пропонує створення кластеру з нереляційними базами даних та контейнеризація самих баз даних, як швидкий, дешевий та надійний спосіб розгорнути середовище.

Кластеризація нереляційних баз даних

Найпопулярнішою робочою моделлю для врівноваження навантаження баз даних NoSQL є заточення (або фрагментація). При фрагментарному підході база даних поділяється на фрагменти (рис. 1), які записують і зчитують дані, що може значно підвищити швидкість роботи з базою даних.

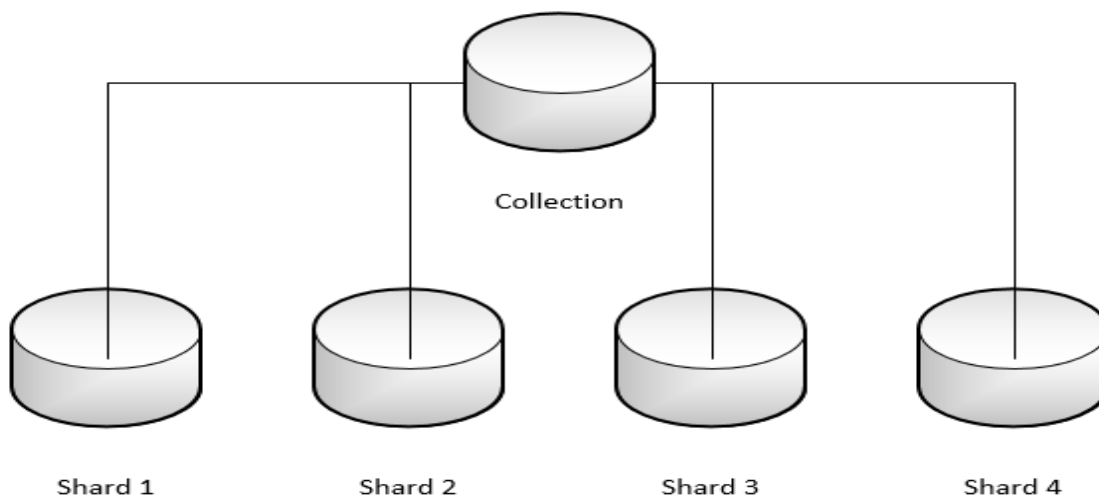


Рис. 1. Узагальнена структура кластерів бази даних, що не мають відношення, на основі дробового типу реплікації.

Алгоритм контейнеризації та управління

У звичайних операційних системах для персональних комп'ютерів комп'ютерна програма може бачити (навіть якщо вона не може отримати доступ) усі системні ресурси. Вони включають:

- Апаратні функції, які ви можете використовувати, такі як процесор та мережеве з'єднання;
- Дані, які можна читати або записувати, наприклад файли, папки та мережеві папки;
- Підключені периферійні пристрої, з якими він може взаємодіяти, наприклад веб-камера, принтер, сканер або факс.

За допомогою віртуалізації або контейнеризації операційної системи ви можете запускати програми в контейнерах, які виділяють лише частини цих ресурсів і не завантажують не потрібних компонентів операційної системи.

Контейнеризація аналогічна віртуалізації додатків: в останньому лише одна комп'ютерна програма розміщується в ізольованому контейнері, а ізоляція стосується лише файлової системи. Тому контейнеризація є перспективним підходом до нашого рішення, оскільки вона дозволить нам налаштувати контейнер найпростішим способом, а потім просто встановити оптимальну кількість контейнерів для збільшення або зменшення необхідних ресурсів.

Це дозволить нашому рішення імітувати фрагменти шардінгу NoSQL з динамічним створенням / видаленням вузлів баз даних. На основі результату, показаного на рис.2, найбільш перспективними базами даних для високонавантажених систем IoT може бути Couchbase.

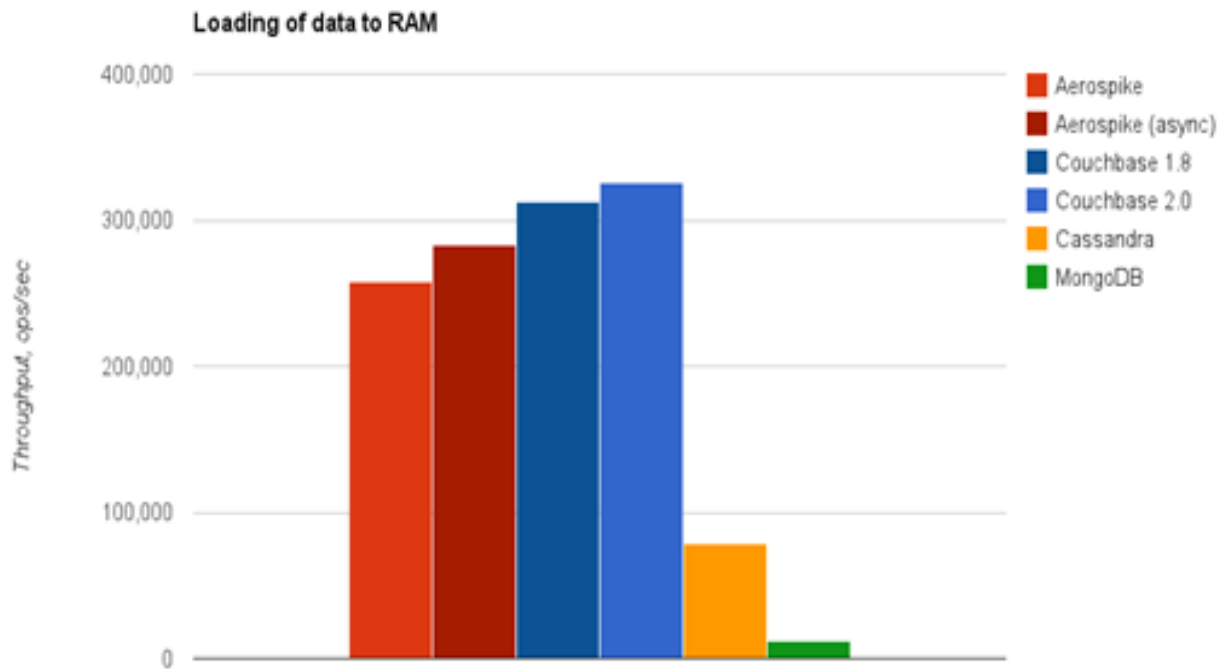


Рис. 2. Завантаження діаграм даних для деяких NoSQL DB.

В якості прикладу візьмемо сервер Couchbase, який може забезпечити 300 000 операцій запису в секунду і мережу, яка може генерувати, наприклад, 200 000 сигналів в секунду з певним граничним коефіцієнтом $\delta = 0,8$, і якщо кількість запитів зростатиме з часом і коли вона досягне до 280 000 запитів в секунду, система розгорне новий контейнер, який буде брати на себе частину навантаження.

А у випадку зменшення трафіку згорне останній і перенесе копію даних на резервну базу.

Висновки. Підсумовуючи вищеописане, для швидкості розгортки та реплікації серверів даних є кілька підходів, які можна об'єднати. Тому наше рішення дозволить розбити систему на автоматизовані контейнери, що будуть працювати по кластерній моделі, що дозволить швидко згорнути і розгорнути додаткові вузли і економити час та гроші замовника.

Література

1. X. Tao and C. Ji, "Clustering massive small data for IOT," The 2014 2nd International Conference on Systems and Informatics (ICSAI 2014), Shanghai, 2014, pp. 974-978. doi: 10.1109/ICSAI.2014.7009427.
2. C. You and X. Wu, "Feature selection embedded subspace clustering with lowrank and locality constraints," 2018 IEEE International Smart Cities Conference (ISC2), Kansas City, MO, USA, 2018, pp. 1-8. doi: 10.1109/ISC2.2018.8656922.
3. H. Hromic et al., "Real time analysis of sensor data for the Internet of Things by means of clustering and event processing," 2015 IEEE International 11 Conference on Communications (ICC), London, 2015, pp. 685-691. doi: 10.1109/ICC.2015.7248401.
4. K. Lin, D. Wang, F. Xia and H. Ge, "Device Clustering Algorithm Based on Multimodal Data Correlation in Cognitive Internet of Things," in IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2263-2271, Aug. 2018. doi: 10.1109/JIOT.2017.2728705.

ПІДХІД ДЛЯ ПОБУДОВИ НЕЧІТКИХ ЛОГІЧНИХ ПРАВИЛ ДЛЯ ВЕЛИКИХ ДАНИХ

Ляшенко А.В.

Інститут телекомунікаційних систем КІП ім. Ігоря Сікорського, Україна

E-mail: andrey.lyashenko44@gmail.com

The approach to building fuzzy logical rules for big data

The article describes how to build fuzzy logic rules after processing and clustering large amounts of data.

У статті наводиться опис побудови нечітких логічних правил після обробки та кластеризації великих обсягів даних.

При проектуванні й розробці реальних смарт-систем з'являється проблема – формування складної математичної моделі, яка буде включати різні технічні особливості обладнання і фізичні характеристики середовища (складні обчислення можуть потребувати додаткові обчислювані ресурси). В ході подальшої розробки, може виникнути потреба врахувати нові умови, що може привести до повної переробки існуючої моделі. В такому випадку, різні умови можна визначати, як деякі правила (ЯКЩО ... ТО), використовуючи нечітку логіку. Для отримання цих правил, можна використовувати експертів, які самі задають умови. А можна навчити систему самій будувати ці правила, використовуючи різні алгоритми кластеризації [1].

Алгоритми кластеризації оперують з об'єктами. З кожним об'єктом X ототожнюється вектор характеристик $X_i = (x_1, \dots, x_d)$. Компоненти X_i , $i = 1, \dots, d$ є окремими характеристиками об'єкта. Розмірність простору характеристик визначає кількість характеристик d . Що складається з усіх векторів характеристик об'єктів, безліч позначається $M = (X_1, \dots, X_n)$. Підмножина «близьких один до одного» об'єктів з M являє собою кластер. Відстань $D(X_i, X_j)$ між об'єктами X_i і X_j визначається в просторі характеристик на основі обраної метрики.

Опис підходу. Суть підходу полягає в тому, що вхідні дані моделюють N -вимірний простір. Якщо змодельовати кожен характеристику об'єкта вхідних даних, як окрему вісь простору, то отримаємо модель в якій, кожен об'єкт цієї вибірки буде знаходитися в цьому просторі. Характеристика об'єкта – це лінгвістична змінна правила. Лінгвістична змінна – це сукупність всіх терм-множин. Терм - опис значення параметра (наприклад температура: холодно, тепло, жарко). Якщо на вхід подається вибірка, яка має тільки дві лінгвістичні змінні, тобто має тільки два стовпця, то вимірний простір – це двовимірний простір. На етапі не ієрархічної кластеризації, обчислюються значення центрів кластерів. Кожен кластер являє собою терм-множину.

P_j	1	2	3	4	5	6	7	8	9
$x=x_1$	0.7	1.4	1.2	1.8	2.5	2.3	2.4	3.0	2.1
$y=x_2$	0.8	0.9	1.3	0.8	0.9	1.6	2.4	2.7	3.0

Рис. 1. Вхідна вибірка.

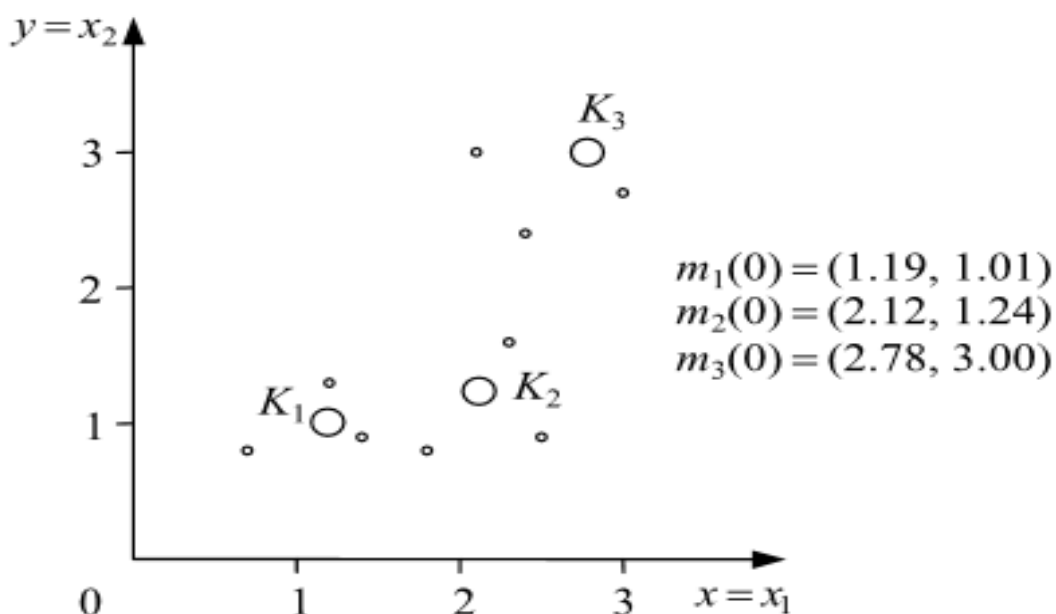


Рис. 2. Двох-вимірний простір, побудований із вхідної вибірки.

При побудові нечітких логічних правил, потрібно визначити функції приналежності. Функції приналежності – це функція, яка по осі ординат має значення від 0 (однозначно належить) до 1 (однозначно не належить), а по осі абсцис – кількісні значення даного терма. Ці функції бувають різних видів: у формі трапеції, трикутна форма, L-функція, R-функція, функція Гаусса. Найлегше можна побудувати функцію Гауса, а вже потім переходити до інших видів.

Функція Гаусса має вид: $\mu(x) = e^{\left(-\frac{(m_{xi}-x)^2}{2\sigma^2}\right)}$, де x – центр кластера, σ – середньо-квадратичне відхилення.

Для знаходження ширини σ скористаємося формулою $\frac{|m_{xi} - m_{x(i+1)}|}{N_x}$, де m_{xi} – центр кластера, $m_{x(i+1)}$ – центр наступного кластера, N_x – кількість кластерів.

Тепер потрібно спроектувати та побудувати на кожну вісь N-вимірного простору, для кожного кластера (терма) функції приналежності Гауссового виду [2].

Після побудови функцій приналежності, потрібно перетворити числові дані, які поступали на вхід, на значення термів лінгвістичних змінних. Кожне числове значення належить якомусь кластеру відповідної лінгвістичної змінної. Відповідно кожен об'єкт із вхідної вибірки, створить окреме нове правило вигляду *Якщо .. Та ... То*. Кожне правило такого типу можна унікально ідентифікувати за набором умов *Якщо*. Під час «мапінгу»

числових даних в терми лінгвістичних змінних, можуть виникати такі умови, коли правила будуть повторюватися. Цей підхід дозволяє уникати таких ситуацій, пропускаючи повторююче правило.

Таким чином, будуються нечіткі логічні правила, для великих обсягів даних.

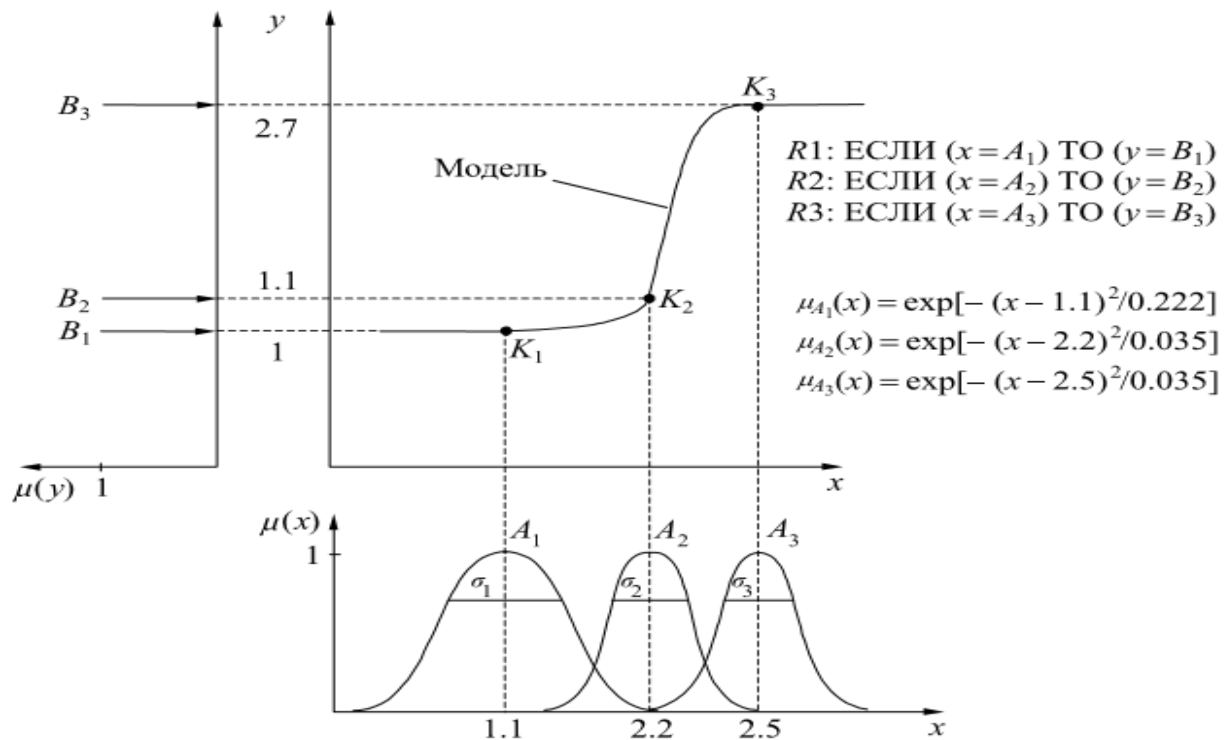


Рис. 3. Побудова функцій приналежності на кожну лінгвістичну змінну.

Висновки. В даній статті був запропонований підхід для побудови нечітких логічних правил для великих даних. Цей підхід базується на моделюванні вхідної відкластеризованої вибірки даних в N-вимірний простір. Кожна вісь цього простору являє собою лінгвістичну змінну, на яку проектується і будується функція приналежності Гауссового виду. Цей підхід допомагає віднести кожне значення об'єкта вхідної вибірки, до відповідного йому терма лінгвістичної змінної і, таким чином, побудувати нечіткі логічні правила, з яких можна створити нечітку базу знань.

В майбутньому планується розробити систему, яка дозволить будувати нечіткі логічні правила, використовуючи даний підхід.

Література

1. Analysis of clustering algorithms for use in the universal data processing system. Larysa Globa, Yurii Buhaienko, Andrii Liashenko, Maria Grebinichenko National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" Kyiv.
2. Нечеткое моделирование и управление. А. Перат с. [506-520].

ЗАСТОСУВАННЯ НЕЧІТКИХ ЛОГІЧНИХ ПРАВИЛ ДЛЯ АНАЛІЗУ ТА СТРУКТУРИЗАЦІЇ ВЕЛИКИХ ДАНИХ

Савчук З.Р., Бугаєнко Ю.М.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: savchukzahar33@gmail.com

Apply fuzzy logic rules for analyzing and structuring Big Data

This article proposes a method that, on the basis of statistics, allows you to build logical structured rules and to test them for accuracy using the apparatus of metagraph theory. The main objective of this article is to structure the base of fuzzy knowledge in the format of logical rules, taking into account the transformation of numerical values into terms of linguistic variables, as well as in the formation of rules to prevent the presence of conflicting and duplicate rules.

В даній статті пропонується метод, який на базі статистичних даних дозволяє будувати логічні структуровані правила і проводити їх перевірку на достовірність за допомогою апарату теорії метаграфа. Головна мета даного підходу полягає в структуризації бази нечітких знань у форматі логічних правил, враховуючи перетворення числових значень у терми лінгвістичних змінних, а також при формуванні правил запобігти наявності конфліктуючих і дублюючих правил.

В останній час тема інтелектуального аналізу даних привернула значну увагу як наукових кіл спеціалістів, так і промисловості. Інтелектуальний аналіз даних – це процес вилучення корисних знань із великих об’ємів даних. Завдяки застосуванню методів інтелектуального аналізу даних розвиваються системи автоматичного отримання знань із статистичних даних. Але однією із складностей такого підходу є те, що якщо система використовується у процесі прийняття рішення, то іноді чітко визначене рішення не завжди може бути правильним. Для того, щоб врахувати можливі граничні умови, застосовують теорію нечітких множин. Саме поєднання теорії нечіткої логіки і методів автоматичного отримання знань статистичних даних є оптимальним варіантом рішення, оскільки вони вирішують проблеми пов’язані не тільки із невизначеністю, але також збільшують виразну силу і зрозумілість класифікаційних знань.

Запропонований метод поєднання побудови бази нечітких логічних правил з перевіркою їх на коректність за допомогою метаграфа дозволяє уникнути дублювання, перетину правил і збільшити якість отриманих результатів, більш чітко визначити зміст логічних зв’язків.

Згідно джерела [1], для звернення з неточно відомими величинами використовувався апарат теорії ймовірностей. Однак в даній ситуації випадковість пов’язана з невизначеністю, що стосується приналежності деякого об’єкту до звичайної множини. І ця різниця між нечіткістю і випадковістю призводить до того, що математичні методи нечітких множин

зовсім не схожі на методи теорії ймовірностей. У цей же час нечітка логіка пропонує нам гнучкість для міркувань, де можна розглянути усі невизначеності будь-якої ситуації, враховуючи приналежність об'єкта до множини.

Підхід на основі теорії нечітких множин є, по суті справи, альтернативою загальноприйнятим кількісним методам аналізу систем. Він має три основні відмінні риси:

- замість або на додаток до числових змінних використовуються нечіткі величини, так звані "лінгвістичні" змінні;
- прості відносини між змінними описуються за допомогою нечітких висловлювань;
- складні відносини описуються нечіткими алгоритмами.

Відповідно до [2] джерела, нечітка логіка базується на узагальненні класичної логіки і теорії нечітких множин, запропонованої американським математиком Лотфі Заде для формалізації нечітких знань, які характеризуються лінгвістичною невизначеністю і призначалась для подолання труднощів уявлення неточних понять, аналізу і моделювання систем, в яких бере участь людина. Такий підхід дає наближені, але в той же час ефективні способи опису систем, які є складними і погано визначеними, у зв'язку з чим не піддаються точному математичному аналізу.

Алгоритм формування правил бази нечітких знань

Як описується в джерелі [3] процедура формування правил обробляє отримані статистичні дані, представленні у вигляді двомірної таблиці. Логічні правила повинні бути представленні у вигляді Якщо .. Та .. То. Кожне правило такого типу можна унікально ідентифікувати за набором умов Якщо. Тобто у системі не може бути двох правил з однаковим набором умов, адже якщо припустити, що такі правила будуть присутніми у системі, то вони або будуть дублювати один одного (у випадку з однаковим результатом) або будуть перечити одне одному (у випадку з різними результатами).

Для перетворення зразку даних у правило та подальшої роботи над ними застосовується підхід, що складається з таких фаз:

- Перетворення числових значень у терми лінгвістичних змінних;
- Формування правил;
- Очищення правил.

У результаті обробки набору правил отримано новий набір, у якому відсутні дублюючі та конфліктуючі правила. Даний набір правил може бути використаний у механізмі логічного виводу.

В даному випадку, найкращим засобом подання нечіткої бази знань є візуалізація графових структур, але на сьогоднішній день ні один із приведених алгоритмів не використовував можливість її подання за допомогою теорії метаграфа. Саме тому виникає доречність та актуальність

створення автоматичної побудови даного засобу, який буде візуалізовувати складні логічні структури. У даному випадку це дозволить наочно редагувати логічні структури, визначати та аналізувати її властивості, які важко виявити, використовуючи текстове або формальне подання [4].

Запропонований об'єднаний метод побудови бази нечітких логічних правил з перевіркою їх на коректність за допомогою теорії метаграфа має такі переваги:

- спрощена процедура формування правил;
- зменшена обчислювальна складність під час формування правил;
- якісна перевірка дозволяє видалити конфлікти, що підвищує достовірність отриманих правил.

Даний механізм можна використовувати в:

- Системах прийняття рішень;
- Системах управління;
- Платформи мережевої конфігурації.

Висновки. В даній статті було проведено аналіз методів та алгоритмів формування бази нечітких логічних правил та запропоновано об'єднаний метод побудови бази нечітких логічних правил з перевіркою їх на коректність за допомогою теорії метаграфа. Даний підхід можна вважати новим продуктивним методом графічного аналізу складних логічних структур, оскільки він дозволяє підвищити якість та достовірність отриманих нечітких логічних правил з візуалізацією у вигляді метаграфа.

Література

1. Алтунин А.Е., Семухин М.В. Модели и алгоритмы принятия решений в нечетких условиях: Тюмень: Издательство Тюменского государственного университета, 2000, ст 4-11.
2. Zadeh L. A. Fuzzy Sets. — Information and Control, 1965, Vol. 8, № 3, pp. 338–353.
3. Захарчук А.Г. «Методи нечіткої логіки для обробки даних в мережі Інтернету Речей», ст 66- 80, Київ 2019.
4. Савчук З.Р. «Засоби візуалізації складних логічних структур», Збірник матеріалів Міжнародної науково-технічної конференції «Перспективи телекомунікацій», Київ 2019.
5. Штогріна О.С., «Інформаційна технологія створення та використання баз нечітких знань із застосуванням метаграфів», ст 35-48, Київ 2016.
6. Nachul S., Jünger M. An Experimental Comparison of Fast Algorithms for Drawing General Large Graphs // LNCS, Springer. 2006. Vol. 3843. – pp. 235 - 250.
7. <https://www.guru99.com/what-is-fuzzy-logic.html>.

СИСТЕМА КОМП'ЮТЕРНОГО ЗОРУ ДЛЯ НАВІГАЦІЇ В ПРИМІЩЕННІ ЛЮДЕЙ З ВАДАМИ ЗОРУ

Остапенко М.С., Штогріна О.С.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: mak7.ostapenko@gmail.com

Computer vision indoor navigation system for vision-impaired people

The problem of indoor navigation of visually impaired people is considered. A navigation system is offered to solve the problem. Proposed a solution to the problem using approaches for indoor robot navigation. In the future, the system will be implemented as a mobile application and a web service.

Проблема підтримки переміщення людей з вадами зору є практично не вирішеною. Хоча й навігація на вулиці можлива за допомогою GPS [1] та тактильних елементів бруківки, але ці методи не дозволяють в повній мірі безпечно взаємодіяти із світом. Це не тільки із-за обмеженості тактильного покриття та похибок GPS, а також із-за обмеженої кількості інформації, яку можна передати через ці джерела. В приміщеннях проблема стоїть ще гостріше. По-перше, в приміщенні похибка GPS може сягати п'яти метрів і більше, а в деяких випадках сигнал відсутній, що унеможливорює його використання. По-друге, більшість приміщень не мають тактильної плитки навіть на першому поверсі, відсутнє дублювання тексту шрифтом Брайля та відсутні тактильні мапи, які дозволяють уявити схему приміщення.

Існуючі технологічні рішення не справляються із проблемою, тому що вони є або дорогими, або незручними у використанні для користувачів. Для прикладу, використання NFC[2] міток чи знаходжень координат мобільного пристрою за допомогою мережі Wi-Fi, в якій він знаходиться, може допомогти орієнтуватись в приміщенні людині з вадами зору. Ці технології є зручними, відносно дешевими та доступними для вирішення поставленої задачі. Однак на ринку немає масового продукту з необхідною функціональністю, який можна просто встановити і користуватись. Тому в роботі стоїть актуальна задача створити систему комп'ютерного зору для навігації людей з вадами зору практично у будь-якому приміщенні.

Розроблювана система повинна задовольняти наступним вимогам:

- безпечність переміщення – визначення чітких меж приміщення, для уникнення нещасних випадків;
- можливість взаємодії із навколишнім світом – визначення місцезнаходження необхідних предметів для уникнення перешкод;

- використання в будь-якому спеціально не пристосованому приміщенні – приміщення не переобладнується заздалегідь, не вимагає зусиль та витрат від власників приміщень для підтримки та впровадження системи;

- масова доступність – використання тільки загальнодоступних приладів та технологій без залучення спеціалізованих приладів;

- простий та зрозумілий інтерфейс взаємодії із користувачем;

- стійкість та надійність при збільшенні кількості користувачів.

При вирішенні поставленої задачі по розробці системи навігації людей з вадами зору у будь-якому спеціально не пристосованому приміщенні доцільно застосувати алгоритми комп'ютерного зору та на їх основі створити мобільний додаток, який можливо широко та швидко поширювати та використовувати з вже наявним у користувача смартфоном.

Припустимо, що користувач зі своїм смартфоном розглядається як агент чи робот із простором можливих дій та набором сенсорів. Це припущення дозволяє вирішувати задачу з точки зору робототехніки. Тому система, як і робот, повинна містити наступні модулі:

- модуль побудови тривимірної мапи простору з потоку двовимірних зображень;

- модуль планування шляху;

- модуль локалізації на мапі;

- модуль розпізнавання об'єктів для можливої взаємодії агента із середовищем;

- модуль знаходження та уникнення перешкод.

Окрім всіх вище згаданих модулів є необхідним інтерфейс взаємодії програми із агентом-користувачем. Модуль взаємодії для агента має забезпечувати:

- ефективний опис навколишнього середовища;

- чіткий набір команд для управління програмою і встановлення мети.

Сучасні смартфони мають необхідні сенсори – акселерометр, гіроскоп та камера, показники з яких виступають основним джерелом вхідної інформації для основних модулів системи. Також смартфони мають достатню обчислювальну потужність для забезпечення роботи вищезгаданих модулів, але у випадку, якщо запропоновані алгоритми будуть на високому рівні оптимізовані по критеріям економного використання обчислювальних ресурсів та управління пам'яттю.

Для забезпечення високої якості знаходження перешкод та розпізнавання об'єктів з потоку кадрів використовуються згорткові нейронні мережі [3]. Після проведеного аналізу, було прийнято рішення

використовувати архітектури типу MobileNet [4], тому що вони є оптимізованими для мобільних пристроїв і мають високу якість роботи. Таким чином, використовуючи алгоритми сегментації цільових об'єктів на зображеннях, можливо робити дослідження середовища та пошук об'єктів, в яких зацікавлений користувач.

Для додавання мапи приміщення в систему необхідними кроками є:

1. Заздалегідь записати відео переміщення по всьому приміщенню, для якого створюється мапа.

2. Завантажити відео в систему, де з нього буде створена мапа навігації.

Робота користувача з системою буде включати наступні кроки:

1. Ініціалізація – агент підходить до будівлі і повідомляє свої GPS координати або адресу будівлі, у відповідь система надсилає мапу приміщення на телефон агента та ініціалізує його на вході.

2. Встановлення цілі – агент встановлює ціль у вигляді адреси кабінету або може увімкнути режим дослідження будівлі.

3. Активна робота системи – агент знаходиться у приміщенні і має робити відео зйомку перпендикулярно підлозі. Використовуючи потік зображень та дані із сенсорів, виконується локалізація агента на мапі.

4. Досягнення цілі – фіксується досягнення агентом цілі та відбувається сповіщення про успішне переміщення до запланованої точки. Після досягнення цілі можна встановити нову або вимкнути систему.

Висновок. В роботі розглянуті проблеми при переміщенні людей з вадами зору по території незнайомого приміщення, висунуті вимоги до системи підтримки навігації у таких умовах. В результаті запропонована система комп'ютерного зору для навігації в спеціально непристосованому приміщенні людей з вадами зору. Описана її архітектура та принцип роботи. Система є простою у використанні та не вимагає залучення додаткових спеціалізованих пристроїв для її впровадження.

Література

1. "GPS: Global Positioning System (or Navstar Global Positioning System)" Wide Area Augmentation System (WAAS) Performance Standard, Section B.3, Abbreviations and Acronyms. [1] Archived April 27, 2017, at the Wayback Machine.
2. Cameron Faulkner. "What is NFC? Everything you need to know". Techradar.com. Retrieved 30 November 2015.
3. A. Krizhevsky, I. Sutskever, and G. Hinton "Imagenet classification with deep convolutional neural networks". InNIPS, 2012.
4. Andrew G. Howard, Menglong Zhu, Bo Chen, Dmitry Kalenichenko, Weijun Wang, Tobias Weyand, Marco Andreetto, Hartwig Adam "MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications". arXiv:1704.04861, 2017.

МЕТОД ВИЯВЛЕННЯ ВПЛИВІВ НА ПСИХОФІЗІОЛОГІЧНИЙ СТАН ЗИМІВНИКА

Куш В. С., Штогріна О. С.

Інститут телекомунікаційних систем КПП ім. Ігоря Сікорського, Україна

E-mail: vetalkushch13@gmail.com

Method of detecting the effects on the psychophysiological state of human

This article describes the load of environmental colors on the psychophysiological state and its interaction with the physiological parameters of the person. Also the method is proposed to detect the effects on the psychophysiological state of various factors, and software has been developed that allows the data visualization settings to be modified on the runtime to obtain multiple image variants.

Україна від початку своєї незалежності проводить наукові дослідження на антарктичній станції «Академік Вернадський». Отримані результати досліджень у різноманітних галузях можуть бути достатньо важливими для розвитку української держави у економічному та наукових напрямках. Дослідниками, зимівниками, на антарктичній станції є видатні українські науковці з багатолітнім досвідом. В результаті проживання в замкнутому колективі та в суворих кліматичних умовах, які суттєво відрізняються від звичного їм середовища, стан зимівників може погіршуватися, що, у свою чергу, сповільнює ведення досліджень на антарктичній станції. Під час перебування на Антарктиді, організм зимівників перебуває не тільки під гнітючим впливом специфічного клімату, а й специфічного кольорового оточення, яке переважно складається з білого кольору. Психологи розробили методи щодо оцінки та коригування психофізіологічного стану людини на основі кольорової преференції [1], які вже неодноразово показали позитивні результати.

Для оцінки психофізіологічного стану зимівників проводять тест преференцій, який складається із дванадцяти кольорових карток [2]. Використовуючи отримані результати, за допомогою методів на основі кольорової преференції, проводяться дослідження та оцінка психофізіологічного стану зимівників. Але не для всіх зимівників ці дослідження показали високу достовірність. Це можна пояснити тим, що дослідження психофізіологічного стану достатньо широка та складна наукова область та використання одного критерія – кольорової преференції, не може забезпечити достатньо високу точність для всіх зимівників. Тому доцільно розробити новий метод дослідження психофізіологічного стану, який спільно із кольоровою преференцією буде враховувати ряд фізіологічних показників зимівників, які фіксуються під час різних навантажень упродовж усієї експедиції. Це дозволить збільшити вірогідність отримання точної оцінки та ефективного коригування стану зимівників в майбутньому. Також на основі запропонованого методу необхідно розробити програмне забезпечення (ПЗ), яке дозволить враховувати всі зафіксовані показники та будувати графіки їх

залежностей для наочного зображення динаміки зміни психофізіологічного стану. Розроблене ПЗ повинно надавати можливість на ходу задавати параметри візуалізації, що у свою чергу дасть можливість психологам отримати декілька варіантів візуалізації, знаходити та відслідковувати нові залежності.

Лікар експедиції під час перебування на антарктичній станції фіксує фізіологічні показники кожного зимівника при різних обставинах. Наприклад, пульс фіксувався у чотирьох станах: у спокої та при навантаженні на велотренажері протягом трьох хвилин на різних потужностях: 50Вт, 100Вт, 150Вт. Також фіксувались дані про вагу зимівників та інші.

Розроблений метод ґрунтується на поєднанні візуалізації на одному зображенні різнорідних даних, наприклад, вище перелічених фізичних характеристик та кольорової преференції. Таке поєднання дає можливість бачити динаміку зміни цих показників, виявляти можливі їх взаємозв'язки та встановлювати їх вплив на психофізіологічний стан. Також він збільшує достовірність оцінки стану зимівників, за рахунок розширення дослідження новими показниками та його поєднання із уже існуючими методами оцінки психофізіологічного стану. Тестування розробленого методу проводилося на основі вибірки отриманих даних про зимівників від НАНЦ України.

Результат використання запропонованого методу продемонстровано на рис. 1. На цьому рисунку відображені залежності фізіологічних характеристик зимівників та кольорової преференції, які згруповано по датам. Фізіологічні показники зображено стовпчиками, висота яких відповідає реальному значенню цього критерія у зазначену дату. Знизу, під стовпчиками фізіологічних показників, кольором зазначена кольорова преференція для відповідної дати. З рисунка можна побачити явне погіршення фізичного фактору зимівника під час початку експедиції. Оскільки, спостерігається різке збільшення тиску під усіма навантаженнями та саме в цей період він мав червону преференцію, що вказує на критичний стан фізичної складової психофізіологічного стану. Але через декілька місяців після початку стан нормалізувався, що говорить про те, що зимівник почав адаптуватися і фізичний стан став наближатися до норми.

Таким чином динаміку зміни фізіологічних показників можна відслідкувати за допомогою зміни рівнів стовпців, а кольорової преференції за допомогою кольорових стовпців – індикаторів, які не створюють додаткової громіздкості. Також психологи мають можливість самостійно задавати конфігурацію через інтерфейс: характеристики, як слід зобразити, масштаб, колір, вказати осі та тип графіку: стовпчики, лінія. Розроблений динамічний механізм візуалізації дозволяє підбирати різні варіації компоновки даних, для виявлення неочевидних залежностей між показниками, та більш наочно прослідковувати критичні моменти та робити відповідні заключення.

Розроблене ПЗ дозволяє забезпечити пошук залежностей між психофізіологічними показниками людини, за рахунок візуалізації даних

різного роду у потрібній формі для наочного дослідження. Для його розробки використано мову програмування С#. Для сховища зібраних даних використано СУБД MS SQL. В ньому зберігаються всі імпортовані дані, також використано механізми індексації, які застосовано до тих областей даних, які часто використовуються, що зменшує час відгуку системи для користувачів та збільшує продуктивність досліджень показників стану зимівників. Також були реалізовані можливості для імпорту та експорту даних в різні формати, наприклад, .xlsx. Що дає змогу швидко занести дані до ПЗ та зберегти резервну копію даних.

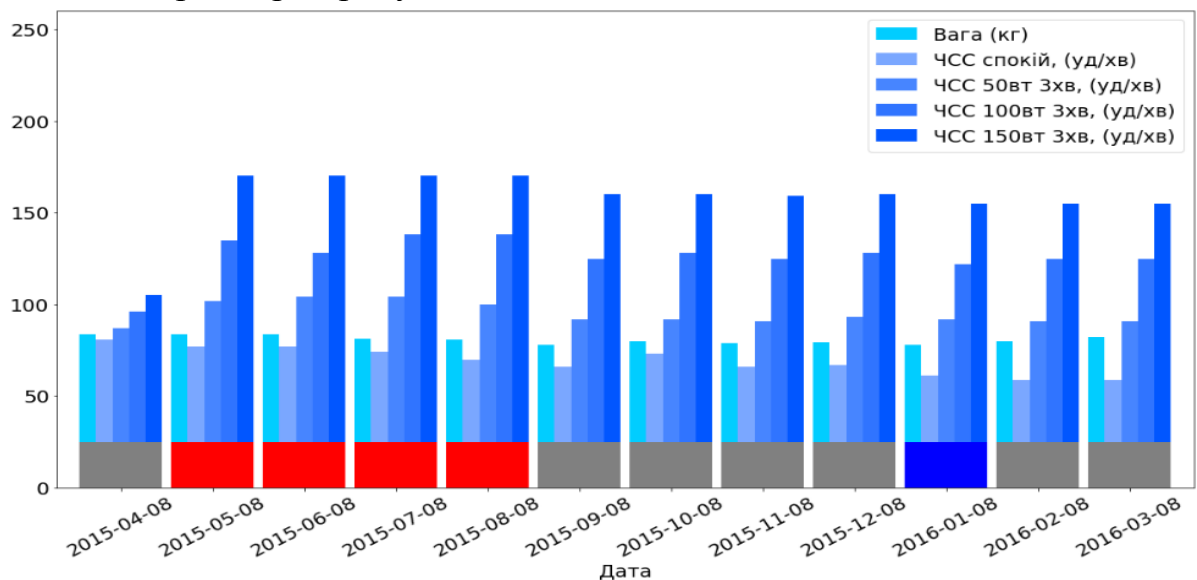


Рис. 1. Приклад частини інтерфейсу користувача:
варіант візуалізації залежностей фізіологічних
характеристик зимівника та кольорової палітри.

В результаті проведеної роботи було розроблено метод, який дозволяє розширити процес дослідження психофізіологічного стану зимівників під час перебування на антарктичній станції базуючись на отриманих даних від НАНЦ України. На основі цього методу розроблено ПЗ, за допомогою якого можна сформулювати декілька можливих варіантів візуалізації даних, використовуючи можливість на ходу задати параметри візуалізації, та обрати для подальших досліджень найбільш показові приклади. В свою чергу, таке рішення дає можливість більш глибоко наочно дослідити динаміку зміни отриманих показників стану людини. Розроблене ПЗ передбачає легку інтеграцію з уже існуючим ПЗ НАНЦ України. Імпортовані результати обстеження зимівників та згенеровані зображення візуалізацій зберігаються в базі даних НАНЦ, тому доступ до них забезпечується з будь якого місця, при наявності доступу до мережі.

Література

1. Мадяр А.Й. Спосіб корекції психофізіологічного стану людини. / А.Й. Мадяр, О.Е. Ковалевська, В.В. Арбатов, В.Н. Бережанський, М.В. Луцюк, Є.В. Моїсенко, С.В. Чорний // Патент на корисну модель №28058 від 26 листопада 2007 року.
2. 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.

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ МЕТОДІВ МОНІТОРИНГУ РУХОМИХ ОБ'ЄКТІВ В СИСТЕМАХ РОЗУМНОГО БУДИНКУ

Могильний С.Б., Мініч М.А.

Інститут телекомунікаційних систем КІП ім. Ігоря Сікорського, Україна

E-mail: isearch@ukr.net, marinka43753@gmail.com

Research of the effectiveness of monitoring methods for moving objects in smart house systems

The article is devoted to the study of algorithms for detecting moving objects in a video sequence. Algorithms based on the OpenCV library that can be applied in low-power systems of the “smart home” and their ability to cope with distortions caused by possible attacks are investigated.

Стаття присвячена дослідженню алгоритмів виявлення рухомих об'єктів на відеопослідовності. Проаналізовано алгоритми, на основі бібліотеки OpenCV, що можуть бути застосовані в малопотужних системах «розумного будинку» та їх здатність протистояти спотворенням, що можуть бути викликані можливими атаками.

У сучасному світі мультимедійні потоки використовуються досить широко в різних секторах економіки виробництва і сферах життя людей. У сфері автоматизації охорони, потрібно використовувати додаткові алгоритми, що дозволяють не тільки передавати і показувати інформацію, що надходить на вхід, але ще й відслідковувати зміни щодо попередніх даних і інформувати про це користувача або вести запис історії таких змін.

Однак, сучасні алгоритми істотно поступаються людині в якості супроводу людей. У зв'язку з цим, їх використання для рішення практичних завдань дуже обмежене. Іншим суттєвим обмеженням є висока обчислювальна складність багатьох алгоритмів аналізу відео, що не допускає їх практичне застосування на сучасному рівні розвитку техніки. Широка доступність відеокамер і розвиток комп'ютерних мереж дозволили створити системи відеоспостереження, які об'єднують понад сотні тисяч камер. Однак навіть алгоритми первинного аналізу такі, як виявлення об'єктів інтересу (людей, машин та ін.), не дозволяють обробляти більше декількох відеопотоків на центральному процесорі або розраховані на дорогі графічні прискорювачі.

На даний момент існує багато різноманітних алгоритмів, що вирішують задачу стеження за об'єктом.[1] Оскільки в системах безпеки для розумного будинку часто застосовують камери з невеликою розрізною здатністю і є обмеження на характеристики, то для підбору оптимального алгоритму, було вирішено зупинитись на бібліотеці OpenCV (Open Source Computer Vision), що включає в собі велику кількість готових алгоритмів, з котрих було обрано ті, що використовуються для стеження за об'єктами: BOOSTING, MIL, KCF, TLD, MEDIANFLOW, GOTURN, MOSSE і CSRT.[3] У роботі не розглядаються алгоритми, що базуються на нейронних мережах та машинному навчанні, таким алгоритмом у обраній бібліотеці є Goturn.

Не менш важливим у застосуванні алгоритму є його показники роботи: швидкодія, точність, здатність працювати у спотворених умовах, таких як підвищена кількість шумів та зміна інтенсивності освітлення кадру, та інші, що відповідають умовам конкретної задачі.[2] У даній роботі було проаналізовано лише показники, що наведені вище, для вибору кращого алгоритму серед представлених.

В таблиці 1 наведено порогові значення (у відсотках), при яких алгоритм починає працювати неправильно. Градація вимірювання точності була складена наступним чином: погана: 0-20%, недостатня: 20-40%, помірна: 40-60%, задовільна: 60-80%, висока: 80-100%.

Таблиця 1. Практичний аналіз роботи алгоритмів за різних умов.

	Boosting	MIL	KCF	TLD	Median-Flow	MOSSE	CSRT
Рівень шумів	96%	95%	60%	60%	60%	35%	75%
Зменшення яскравості, кольорове зображення	1%	1%	17%	10%	20%	17%	17%
Збільшення яскравості, кольорове зображення	99%	99%	83%	87%	89%	83%	91%
Зменшення яскравості, чорно-біле зображення	1%	1%	20%	30%	15%	11%	1%
Збільшення яскравості, чорно-біле зображення	99%	99%	64%	82%	90%	85%	82%
Середнє значення швидкодії (FPS, кадр за секунду)	32	12	42	9	146	178	25
Точність знаходження об'єкта	Висока	Висока	Помірна	Недостатня	Висока	Висока	Недостатня

З таблиці 1 видно, що в умовах з низьким або з високим рівнем освітленості задовільною є робота декількох трекерів. Проте найкращі результати показали Boosting та MIL. Найбільш швидкими для застосування в умовах реального часу виявились – MedianFlow та MOSSE. Найточніше відстеження об'єкта реалізують – Boosting, MIL, MedianFlow, MOSSE. Алгоритми Boosting та MIL краще з усіх виявляють об'єкт при високому рівні шумів.

Для задоволення умов поставленої задачі алгоритм повинен мати: швидкість зміни кадрів - не менше 30; точність знаходження об'єкта – не менше 50%; відстеження об'єкта при рівні шумів – не нижче 60%; зміна освітлення – в межах 20% - 80%.

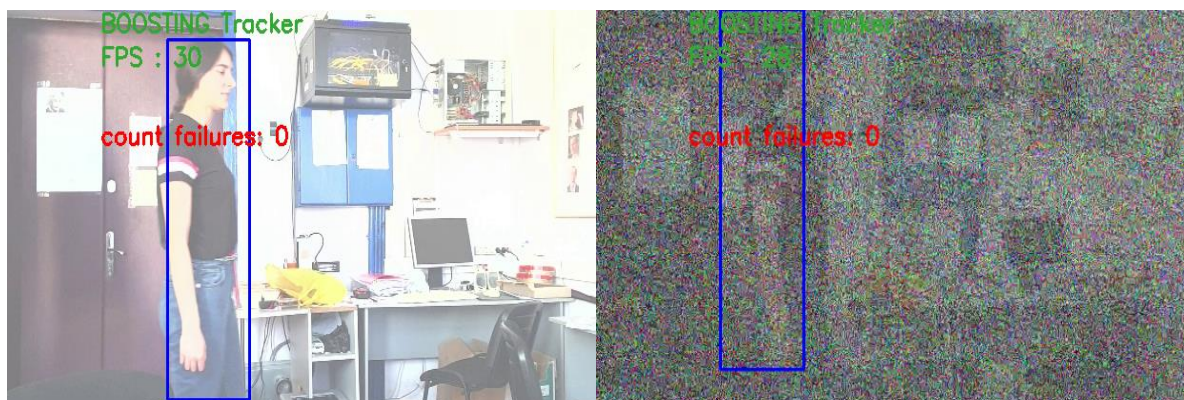


Рис. 1. Результати роботи BOOSTING при збільшеній освітленості кадру та при збільшеному рівні шумів у кадрі відповідно.



Рис. 2. Результати роботи MedianFlow при збільшеній освітленості кадру та при збільшеному рівні шумів у кадрі відповідно.

Беручи до уваги наведені вище умови, можна зробити висновок, що для вирішення даної задачі можна використовувати алгоритми Boosting або MedianFlow. Нижче наведені рисунки роботи алгоритмів при погіршених умовах передачі зображення.

Література

1. Adrian Kaehler, Gary Bradski. Learning OpenCV 3: Computer Vision in C++ with the OpenCV Library, p.875.
2. Adrian Rosebrock. Simple object tracking with OpenCV: Веб-ресурс - <https://www.pyimagesearch.com/2018/07/23/simple-object-tracking-with-opencv/>
3. Amin Ahmadi Tazehkandi. 2018. Computer Vision with OpenCV 3 and Qt5, p.200.

АНАЛІЗ ОЦІНКИ ЯКОСТІ НАДАННЯ ПОСЛУГ ТЕЛЕКОМУНІКАЦІЙНИМ ПРОВАЙДЕРОМ

Глоба Л.С., Попова М.А., Юшко Н. А.

Інститут телекомунікаційних систем

E-mail: Lgloba@its.kpi.ua, pma1701@gmail.com, natalia.yushko@outlook.com

The approach to quality control of telecommunication service providers

The modern development of telecommunications and telecommunication providers requires an increasing level of service provision, because the formation of a market for network services has increased attention to issues of quality control, both by regulators and by providers themselves. To ensure compliance with the specified level of quality of service provision, telecommunication operators themselves develop algorithms and solutions to control the quality of service provision, based on different criteria. However, these solutions are not universal to different types (quantitative, qualitative, etc.) of service quality indicators. So, **the main purpose** of this work is to present improved approach to quality control of telecommunication service providers. The implementation of the proposed approach is performed using the ontological model of service quality indicators provided by the provider and the dynamically changing workflow, which provide versatility and automation of quality control of service delivery process.

У сучасному світі все більше зростає кількість провайдерів, що постачають послуги різного типу: від доступу до Інтернету та телефонії, до провайдерів контенту, over the top сервісів тощо. Таке зростання пояснюється тим, що цифрові сервіси наразі набувають все більшої актуальності та затребуваності, а конкуренція в середовищі зростає. І саме це спричиняє необхідність вираховувати та обчислювати якість надання послуг, стандартизувати її, та відповідати нормам що диктує конкурентне середовище. З огляду на те, що на якість обслуговування впливає багато чинників, що пов'язані між собою різноманітним чином, виникає необхідність автоматизації цього процесу [1,2].

Автоматизувати процес аналізу якості телекомунікаційних послуг запропоновано шляхом формування та виконання workflow, який генерується з онтології області дослідження. Це дозволить зробити алгоритм обчислення більш інкапсульованим, а отже, простішим для використання кінцевим користувачем без додаткових витрат на програмування для економії матеріальних та часових ресурсів.

Виходячи із попередніх досліджень [3,4,5,6], метою роботи є розробка макету (прототипу) платформи для виконання складних обчислювальних сценаріїв шляхом узгодженої взаємодії веб-сервісів (мікросервісів) на основі сервіс-орієнтованої (мікросервісної) архітектури з використанням онтологічної бази знань [7,8]. У якості моделі даних предметної області запропоновано онтологічну модель даних, яку можливо представити у вигляді деревоподібної структури. В загальному випадку онтологію деякої предметної області формально представляють впорядкованою трійкою:

$$O = \{X(w, s, r), R(w, s, r), F\} , \quad (1)$$

де X, R, F – кінцеві множини відповідно: X – множина реєстрів (Xw – реєстр воркфлоу, Xr – реєстр запитів, Xs – реєстр сервісів) , R – множина відношень між

реєстрами, F – множина функцій інтерпретації X та/або R .

Онтологічна структура дозволяє працювати із різнорідними, неструктурованими даними. Наприклад, для побудови платформи для оцінки якості надання послуг телекомунікаційним провайдером визначено чотири основних реєстри: реєстр послуг; реєстр мікросервісів; реєстр workflow; реєстр запитів.

Реєстр послуг – онтологічна структура, що містить у собі перелік усіх послуг, що надаються телекомунікаційним провайдером. У даному реєстрі класифіковано основні послуги провайдера: поділено їх на класи (Internet, TV, OTT), рівень сервісу (top lever offerings, second level offerings), вказано характеристики сервісу, тип користувачів, допустимі значення, тощо.

Реєстр мікросервісів – онтологічна структура, що представляє собою дерево із сервісів, які будуть використовуватись для обчислення складних технічних параметрів. Для опису кожного мікросервісу використовувалась математична модель, що представлена у вигляді формули (5):

$$M_i = \{Ip_{i..j}, Op_{i..j}, A_i, T_i, P_{i..j}\}, \quad (2)$$

де $Ip_{i..j}$ – вхідні дані що потрібні для роботи мікросервіса; $Op_{i..j}$ – вихідні дані; A_i – алгоритм мікросервісу; T_i – тип вихідних даних мікросервісу (кількісний, логічний); P_i – процеси, що обов'язково повинні бути виконані до даного мікросервісу.

Реєстр workflow – це онтологічна структура, що містить у собі набір обчислювальних сценаріїв для виконання workflow з описаними параметрами. Для опису кожного workflow застосовується математична модель представлена у формулах 6, 7, 8.

$$W_i = \{Ip_w, Op_w, D_w, Dg_w, Pr_w\}, \quad (3)$$

де Ip_w – вхідні дані для workflow; Op_w – вихідні дані workflow; D_w – короткий опис діаграми; Dg_w – BPMN діаграма, що пов'язана з даним workflow та є його графічною репрезентацією; Pr_w – пріоритет виконання workflow.

$$Ip_w = \bigcup_{M_n}^{M_k} Ip_{i..j}, \quad (4)$$

де Ip_w – вхідні дані для workflow представляється об'єднанням всіх вхідних параметрів $Ip_{i..j}$ по всім мікросервісам $M_n \dots M_k$.

$$Op_w = \bigcup_{M_n}^{M_k} Op_{i..j}, \quad (5)$$

де Op_w – вхідні дані для workflow представляється об'єднанням всіх вихідних параметрів $Op_{i..j}$ по всім мікросервісам $M_n \dots M_k$.

Реєстр запитів – це онтологічна структура запитів, що представлена у вигляді опису запитів, та відповідних їм workflow. Математична модель реєстру запитів представлена у формулі (9).

$$R_i = \sigma_c(W_i), \quad (6)$$

де R_i – запит, що має бути введений користувачем, σ_c – функція вибірки відповідного workflow по умові C , W_i – відповідний workflow. Тобто, кожен запит співставлений із відповідним workflow та викликає його виконання.

На Рисунку 1 зображена діаграма послідовностей для описаного процесу.

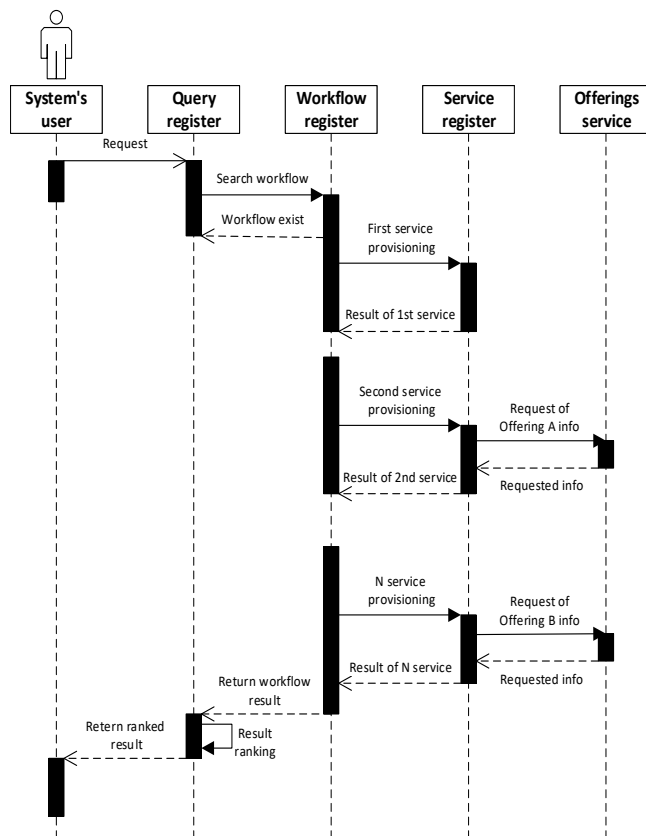


Рисунок 1. Діаграма послідовностей реєстрів сервісів.
предметної області, логічних правил, сервісів, які встановлюють зв'язки між функціональними сервісами.

Література

1. Monograph / [L.S. Globa, M.A Popova, S.O Dovhii, etc.] // Computer ontologies and their use in the educational process. Theory and Practice. / [L.S. Globa, M.A Popova, S.O Dovhii, and others]. - Kyiv, 2013. p. 47-90
2. L.S. Globa Means of access to sources of knowledge and their use in the educational process / L.S. Globa, T.I. Andrushchenko, S.O. Dovhii. // Second edition, supplemented. - 2012.
3. Globa L. S. Integration of ontology-based databases and knowledge bases / L. S. Globa, O. S. Shtogrina, M. Y. Ternovoy. // Collection of scientific works of NTUU "KPI". – 2011. – №1.
4. Globa L. Increasing web services discovery relevancy in the multi-ontological environment / L. Globa, M. Kovalskyi, S. Oleksandr. // Springer, Cham. – 2015. – С. 335–344.
5. Koval A. The approach to web services composition / A. Koval, L. Globa, R. Novogrudska. // Springer international publication AG. – 2017. – №534. – С. 293–304.
6. Popova M. The Formation of Virtual Educational and Research Environment for Distant Education on the Basis of Introduction of Geo-Information System (GIS) Technology / M. Popova. // International Conference Abstracts of Main Speeches ["Ukraine and Montenegro: Present and Perspectives"], (Kyiv, 16 – 19 october 2012) / National Academy of Sciences of Ukraine, National Academy of Pedagogical Sciences of Ukraine, Montenegrin Academy of Sciences and Arts.
7. G Budin (2005), "Ontology-driven translation management", in Helle V. Dam (ed.), Knowledge Systems and Translation, Jan Engberg, Heidrun Gerzymisch-Arbogast, Walter de Gruyter, p. 113, ISBN 978-3-11-018297-2
8. Oberle, Daniel (2014). "How ontologies benefit enterprise applications". Semantic Web. IOS Press. 5 (6): 473–491. doi:10.3233/SW-130114.

Висновки. Даний підхід є універсальним та враховує особливості предметної області, адже замінивши мікросервіси та воркфлоу на будь-які інші та описавши їх взаємозв'язки за допомогою онтологій - система буде в змозі вичислити інші показники та виконати їх ранжування відповідно до зазначених критеріїв. Даний підхід забезпечує інкапсульованість, що в свою чергу спрощує роботу із системою та зменшує ризик помилки у розрахунках. Запропонований підхід автоматизує проектування бізнес процесів та їх складових (мікросервісів, зв'язків та правил взаємодії) шляхом автоматизованої генерації набору сервісів, які є компонентами робочих процесів, а також автоматизує послідовність ості їх виконання за рахунок використання онтології – мета-моделі робочого процесу,

ФОТОМЕТРИЧНА СИСТЕМА ВИМІРЮВАННЯ ПАРАМЕТРІВ ГАЗІВ ТА РІДИН

Адаменко І.О., Губар В.Г.

Факультет електроніки КПІ ім. Ігоря Сікорського, Україна

E-mail: ira_adamenko@ukr.net, s.gubar@kpi.ua

Photometric system for measuring gas and liquid parameters

As of today, there is a large number of optical methods applications for measuring of object's parameters. During the passage of electromagnetic radiation through a solution or dispersed medium, part of the light flux is spent on absorption, reflection and scattering in the substance. The proposed model of device for measuring of the size and amount of impurities has an increased sensitivity of the equipment. Also, in the aforementioned model, the source of electromagnetic radiation and the photodetector are on the same straight line, forming the first channel for measuring the intensity of the output light flux. An additional photodetector forms a second channel, where the scattering intensity is determined. Comparison of values obtained through two channels with the reference gives the final result.

Під час проходження електромагнітного випромінювання через розчин або газ, частина світлового потоку витрачається на поглинання, віддзеркалювання та розсіювання у речовині. Оптичні методи вимірювання [1], а саме турбідиметричний, нефелометричний, абсорбційної фотометрії широко використовуються у хімічних, харчових, машинобудівних, медичних галузях.

У більшості випадків вимірювання параметрів дисперсного середовища базуються на одному з обраних методів. Оскільки, для різних видів домішок, які і визначають основні параметри досліджуваного зразка, треба використовувати різні принципи дослідження. Це пов'язано, у першу чергу, з фізичними властивостями, оскільки поведінка світлового променя буде визначатись, насамперед, довжиною хвилі освітлювача та розміром домішок. Наприклад, молекулярні розчини містять частки розміром менше 10^{-9} м. Грубодисперсні - розмір часток більше 10^{-6} м. Середньої дисперсності 10^{-6} - 10^{-7} м. Колоїдні дисперсні системи містять домішки 10^{-7} - 10^{-9} м. Для кожного випадку використовується різна апаратура.

Головною метою даної роботи є створення універсальної оптичної системи, яка дозволить визначати кількість та параметри домішок у всьому можливому діапазоні.

Проаналізувавши існуючі фотоколориметри, спектрофотометри [2], нефелометри [3] можна визначити основні недоліки:

- суб'єктивна оцінка оптичного коефіцієнту пропускання об'єкта контролю, що пов'язана із візуальною оцінкою рівності світлових потоків вимірювального і компенсаційного каналів;
- похибка на основі освітленості, що створена сторонніми джерелами;
- наявність постійних засвічувань при вимірюваннях, що значно знижує точність результатів;
- втрата світла в системі формування світлового потоку та у

вимірювальній камері;

- обмежений діапазон виміру змісту речовин.

Поєднання декількох методів вимірювань, а саме вимірювання інтенсивності вихідного променя, розсіяного та поглиненого світла, модуляції світлового потоку, розширення кількості каналів вимірювань, використання конструктивних елементів, які містять освітлювач та приймач, на кожній площині кювети зі спрямованою характеристикою випромінювання в різних областях видимого спектра.

Принцип дії полягає у наступному (Рис.1).

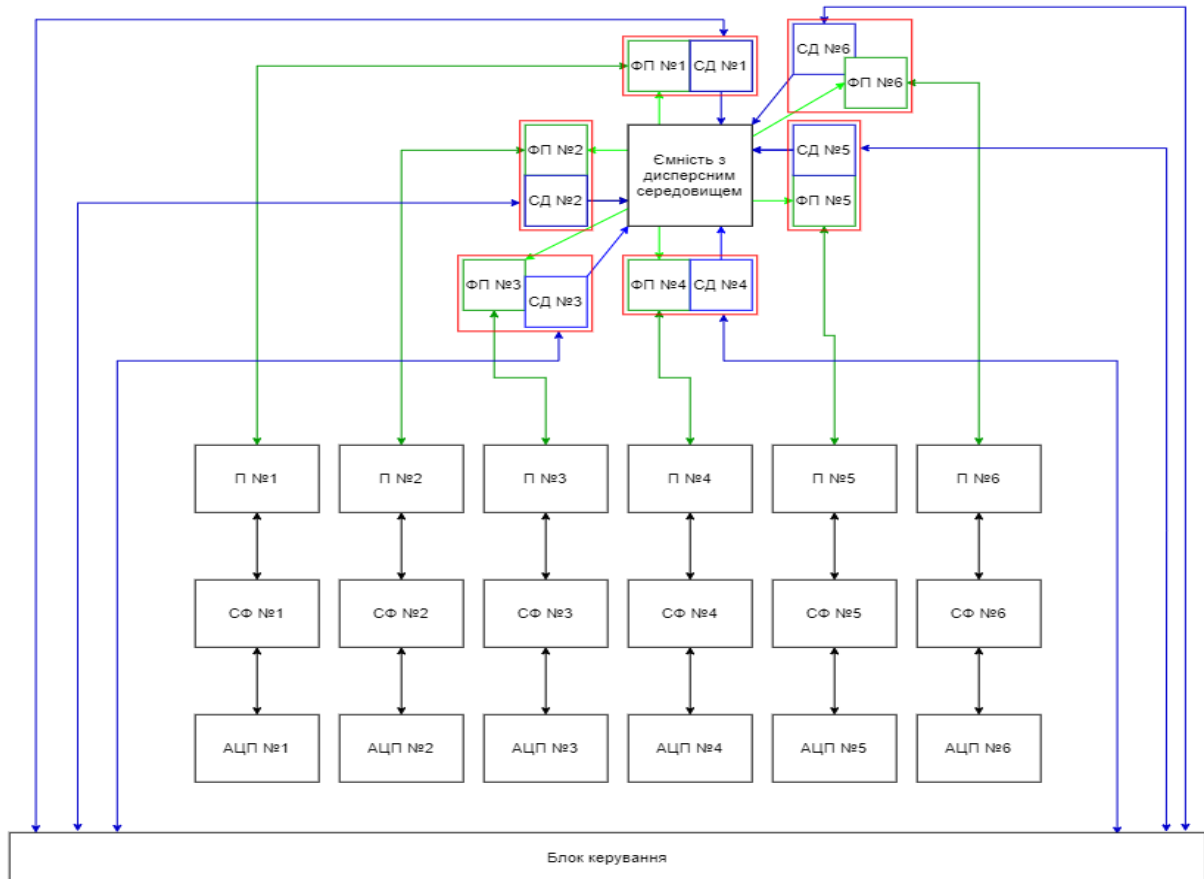


Рис.1. Модель пристрою для визначення розміру та концентрації домішок.

Фотометрична система містить:

- фотоприймач (ФП)
- 4 світлодіоди (СД)
- ємність з досліджуваною рідиною
- підсилювач (П)
- смуговий фільтр (СФ)
- аналого-цифровий перетворювач (АЦП)
- блок керування

Конструктивні елементи, які мають відокремлені і захищені один від одного освітлювальний елемент (4 світлодіоди, різних кольорів) та фотоприймач працюють парами та запускаються блоком керування у визначені часові проміжки, з визначеною частотою.

Перший режим – вимірювання інтенсивності вихідного променя.

Використовуються пари конструктивних елементів, які знаходяться один навпроти другого (№1 та №4; №2 та №5; №3 та №6). Другий режим – вимірювання розсіяного світла. У цьому режимі використовуються усі інші пари конструктивних елементів, які розташовано під прямим кутом один до одного.

В якості джерела світла використовуємо 4 світлодіоди (червоного, синього, зеленого, фіолетового кольорів) та оптичний вузол, який формує на виході чіткий паралельний промінь світла, направлений на ємність з рідиною. Окремий для кожного оптичного каналу таймер генерує коливання з заданою частотою, які з виходів мікроконтролера поступають на освітлювач. Світлові коливання з блоку монохроматичних освітлювачів йдуть на бокову поверхню ємності з досліджуванним середовищем, яке містить домішки, концентрацію та розмір яких потрібно дослідити.

Сигнали з фотоприймачів підсилюються окремими операційними підсилювачами та передаються на смугові фільтри, які виділяють задану частоту. Фільтр складається з двох послідовно ввімкнутих смугових фільтрів, які прибирають стороннє освітлення. Таким чином, пристрій сприймає саме те світло, яке йде з необхідного освітлювача. Отримані сигнали потрапляють на входи аналого-цифрових перетворювачів. З кожного каналу відбувається зчитування значень вимірювань й виконується накопичення змінних. Результат вимірювання розраховується як середнє значення з усіх вимірів.

Мікроконтролер виконує обробку значень, а саме - порівняння результатів отриманих з обох режимів з еталонним значенням. Кінцевий результат надходить на блок інтерфейсу, для зчитування оператором.

Висновок. Запропонована модель фотометричної системи має збільшену чутливість приладу, яка обумовлена використанням освітлювача та фотоприймача з різною довжиною хвилі. У першому режимі джерело електромагнітного випромінювання та фотоприймальний пристрій знаходяться на одній прямій, для вимірювання інтенсивності вихідного світлового потоку. Таке розташування дає змогу зменшити втрати світла, які виникають при встановленні джерела та приймача під кутом 90^0 . Вимірювання у другому режимі, коли освітлювач та фотоприймач знаходяться під кутом 90^0 , визначає інтенсивність розсіювання. Порівняння значень отриманих по двом каналам з еталонним дає кінцевий результат.

Література

1. Карякин А. В., Грибовская И. Ф. Методы оптической спектроскопии и люминесценции в анализе природных и сточных вод, Москва : Химия, 1987, с. 304.
2. Щупляк И. А. Спектрофотометр. СФ-46, Ленинград, 1992.
3. Багатоканальний вимірювач інтенсивності світлового потоку: пат. 123116 Україна. № 201708720; заявл. 29.08.2017; опубл. 12.02.2018, Бюл. № 3
4. Chanson H., Takeuchi M., Trevethen M. Using turbidity and acoustic backscatter intensity as surrogate measures of suspended sediment concentration in a small subtropical estuary, 2007. DOI: 10.1016/j.jenvman.2007.07.009
5. Гершун А. А. Теория светового поля: Избранные труды по фотометрии и светотехнике. ИТМО:Годы и люди: Часть первая, СПб., 2000, с. 284.

СТРУКТУРНО-ФАЗОВОЕ УКРУПНЕНИЕ СОСТОЯНИЙ КОММУНИКАЦИОННЫХ СЕТЕЙ В ЗАДАЧАХ ОЦЕНКИ ХАРАКТЕРИСТИК ДОСТУПНОСТИ СЕТЕВОЙ УСЛУГИ

Зайченко Ю.П., Васильев В.И., Вишталъ Д.М., Любашенко Н.Д.

КПИ им. Игоря Сикорского

E-mail: d.vishtal@kpi.ua

Structurally-phase integration of communication network status conditions in problem of estimation of characteristics of network service availability

Questions of structurally-phase integration of big dimension communication networks with complex structural organization are considered. Characteristics of quality and efficiency of functioning of a network depend on structure of a network and weight parameters of elements.

Структурно-параметрическое моделирование и анализ характеристик доступности сетевой услуги затруднен чрезмерно большим числом возможных различных состояний, что приводит к практической необозримости модели. Идея преодоления этой проблемы состоит в разбиении пространства состояний на конечное число непересекающихся классов, число которых не слишком велико. Функционирование сети в этом укрупненном пространстве состояний описывается без существенных потерь в точности оцениваемых характеристик.

В случае, когда число классов разбиения чрезмерно велико, конструктивным образом строятся оценки сетевых характеристик “снизу и сверху”.

Для сетей со сложной структурной организацией, состоящей из многих элементов, отказ отдельных элементов, в силу структурной избыточности, необязательно приводит к отказу в предоставлении сетевой услуги. Для оценки качества и эффективности функционирования коммуникационных сетей используется следующий набор показателей: стационарная вероятность доступности сетевой услуги; среднее стационарное время доступности (недоступности) сетевой услуги.

Доступность сетевой услуги является универсальной характеристикой, используемой как поставщиками услуг так и пользователями.

В качестве статической модели сети рассматривается размеченный конечный связный неорграф $G(Y;X)$ без петель, где $|Y|$ - число узлов графа, $|X|$ - число ребер графа. Узлы графа играют вспомогательную роль. Матрица смежности узлов графа используется для нахождения представления детерминированных графовых свойств соответствующими структурными функциями.

В качестве динамической модели сети рассматривается стохастический граф, элементы которого взвешены весовыми параметрами. Пространство состояний стохастического графа W_G можно рассматривать и как векторное пространство по $mod(2)$ [1] и как булеву векторную решетку B_2 . Использование пространства W_G удобно для алгоритма нахождения разрезающих множеств графа, циклов, остовов. Векторное пространство W_G содержит два ортогональных подпространства циклов и разрезов, размерность которых равна соответственно цикломатическому числу и рангу графа. Сеть предназначена для обеспечения сетевой услуги в любой момент времени для всех пар узлов. Произвольная пара узлов может получить сетевую услугу, если в данный момент времени найдется по крайней мере один простой путь, их соединяющий. Сетевая услуга доступна для всех узлов, если в данный момент времени существует, по крайней мере, одно остовное дерево.

Элементы сети и структурные функции, соответствующие условиям доступности сетевой услуги, принимают бинарные значения. Пусть $\varphi(x_1(t)...x_n(t))=\varphi(t)$ —

детерминированная структурная функция случайных величин, соответствующая некоторому виду сетевой услуги. Случайная величина $x_i(t)$ ($i=1, \dots, n$) равна 1, если в момент t i -й элемент доступен для выполнения сетевой услуги и равна 0 – в противном случае. Функция $\varphi(t)$ равна 1, если в момент t сетевая услуга выполнима и 0 – в противном случае.

Изоморфизм булевой алгебры классов и соответствующей булевой алгебры свойств дает возможность алгебраизации необходимых вычислений для оценки характеристик доступности сетевой услуги. Функционирование сети рассматривается как процесс случайного блуждания по булевой векторной решетке.

Принятые допущения модели:

- 1) Статистической зависимостью на уровне отдельных элементов можно пренебречь.
- 2) Эволюция элементов моделируется во времени соответствующими альтернирующими процессами восстановления с конечными средними значениями интервалов доступности (недоступности) для выполнения сетевой услуги [2].
- 3) Вектор состояния элементов однозначно определяет состояние доступности (недоступности) сетевой услуги.

$$4) \text{ Существует } \lim_{t \rightarrow \infty} P\{x_i(t)=1\} = \frac{M\theta_i}{M\theta_i + M\xi_i} = P_i, \quad \text{где } M\theta_i, M\xi_i - \text{средние}$$

стационарные интервалы доступности (недоступности) i -го элемента для выполнения сетевой услуги.

- 5) Пространство состояний элементов рассматривается как булева векторная решетка [3].

- 6) В качестве критериального пространства сети рассматривается множество всех изотонных отображений булевой векторной решетки в множество B_2 [3].

Условия независимости функционирования элементов и существования вероятностей $P_i, i=1, \dots, n$ определяют существование и единственность вероятностной меры на булевой алгебре всех подмножеств булевой векторной решетки.

В этих условиях требуется оценить точно или приближенно следующие сетевые характеристики:

$h_\varphi(P_1, \dots, P_n)$ – стационарная вероятность доступности сетевой услуги;

$M\theta_\varphi, M\xi_\varphi$ – средние стационарные интервалы доступности (недоступности) сетевой услуги.

Основная вычислительная проблема оценки сетевых характеристик обусловлена сложностью структурной организации сети и большой размерностью пространства состояний. Это обстоятельство влечет трудновычислимость сетевых характеристик. Можно на несколько порядков поднять порог точной порог точной вычислимости сетевых характеристик, используя декомпозицию структурной функции, свойство дуальных автоморфизмов булевой алгебры и алгоритмы представления структурной функции в ортогональной неповторной форме. Декомпозиция структурной функции позволяет осуществить структурно-фазовое укрупнение состояний сети [4,5].

Детерминированные свойства монотонных структурных функций однозначно определяются следующими МДНФ (МКНФ)-формульными тождествами:

$$\bigvee_{\{\alpha_i\} \in I} (\bigwedge_{k_i \in \{\alpha_i\}} x_{k_i}) = \varphi(x_1, \dots, x_n) = \bigwedge_{\{\beta_j\} \in J} (\bigvee_{r_j \in \{\beta_j\}} x_{r_j}) \quad (1)$$

$$\bigvee_{\{\beta_j\} \in J} (\bigwedge_{r_j \in \{\beta_j\}} x_{r_j}) = \varphi^*(x_1, \dots, x_n) = \bigwedge_{\{\alpha_i\} \in I} (\bigvee_{k_i \in \{\alpha_i\}} x_{k_i}) \quad (2)$$

$$\bigvee_{\{ \beta_j \} \in J} (\bigwedge_{r_j \in \{ \beta_j \}} \overline{x_{r_j}}) = \overline{\varphi(x_1, \dots, x_n)} = \bigwedge_{\{ \alpha_i \} \in I} (\bigvee_{k_i \in \{ \alpha_i \}} \overline{x_{k_i}}) \quad (3)$$

$$\bigvee_{\{ \alpha_i \} \in I} (\bigwedge_{k_i \in \{ \alpha_i \}} \overline{x_{k_i}}) = \overline{\varphi^*(x_1, \dots, x_n)} = \bigwedge_{\{ \beta_j \} \in J} (\bigvee_{r_j \in \{ \beta_j \}} \overline{x_{r_j}}) \quad (4)$$

где $k_i \in \{ \alpha_i \} \wedge x_{k_i} = \alpha_i(x)$ – i -я простая импликанта функции $\varphi(x)$,

$\{ \alpha_i \}$ – набор индексов существенных переменных i -ой импликанты,

$r_j \in \{ \beta_j \} \wedge x_{r_j} = \beta_j(x)$ – j -я простая импликанта двойственной функции $\varphi^*(x)$,

$\{ \beta_j \}$ – набор индексов существенных переменных j -ой импликанты,

$k_i \in \{ \alpha_i \} \wedge x_{k_i} = \alpha_i^*(x)$ – двойственная по отношению к $\alpha_i(x)$ функция,

$r_j \in \{ \beta_j \} \wedge x_{r_j} = \beta_j^*(x)$ – двойственная по отношению к $\beta_j(x)$ функция.

Интерпретация остальных компонент тождеств определяется аналогично.

Символ I используется и для обозначения полного списка простых импликант функции $\varphi(x)$ и для обозначения индексов семейств существенных переменных простых импликант. Символ J используется аналогичным образом.

Сделаем несколько замечаний:

1. Тождества (1-4) дают возможность находить минимальное по числу литералов МДНФ (МКНФ)-представление соответствующих структурных функций. Однако при этом утрачивается независимость функционирования, рассматриваемая на уровне простых импликант функций. В общем случае простые импликанты не являются независимыми случайными величинами.

2. Тождества (1-4) верны не только для бинарных значений переменных, но и для непрерывных неотрицательных значений переменных. С комбинаторной точки зрения теоретико-множественные семейства индексов простых импликант

$I = \{ \{ \alpha_i \} \}_{i=1}^{|\mathcal{I}|}$ и $J = \{ \{ \beta_j \} \}_{j=1}^{|\mathcal{J}|}$ образуют два двойственных семейства минимальных трансверсалей.

3. Знание $M\theta_i$, $M\xi_i$, а также семейств множеств I и (или) J дает возможность выявить “узкие места” в обеспечении сетевых характеристик, определять степень влияния на эти характеристики, как отдельных элементов, так и определенных конфигураций элементов, что важно для развивающихся сетей.

Для оценки характеристик сети используются эффективные алгоритмы поиска семейств I и J , а также алгоритмы декомпозиции структурной функции в ортогональной неповторной форме. С этой целью используется разложение Шеннона и, при необходимости, обобщенные формулы Де Моргана. В работе рассматриваются иллюстративные примеры оценки сетевых характеристик в зависимости от весовых параметров элементов и разных структурных функций.

Литература

1. М. Свами, К. Тхуласираман. Графы, сети и алгоритмы. - М.: Мир - 1984.- 455 с.
2. К. Райншке, И. Ушаков. Оценка надежности систем с использованием графов.- М.: Радио и связь - 1988.- 208 стр.
3. Г. Биркгоф. Теория решеток - М.: Наука, 1984.
4. Г. Биркгоф, Т. Барти. Современная прикладная алгебра.- М.: Мир - 1976.
5. Р. Сикорский. Булевы алгебры. - М.: Мир - 1969.- 375 с.

КОМПОНЕНТНА КОНФІГУРАЦІЯ КОГНІТИВНИХ СЕРВІСІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ ПРИЙНЯТТЯ РІШЕННЯ

Подліпасєв В.О., Чепков Р.І.

Інститут телекомунікацій і глобального інформаційного простору

НАН України, Україна

E-mail: pva_hvu@ukr.net

Component configuration of cognitive services to make a decision

The features of geoinformation support for decision-making process using heterogeneous sources that contain unstructured or poorly structured data are investigated. Cognitive services that provide specific processes of geospatial analysis and are transdisciplinary are analyzed. The conceptual components (targets) of data processing are defined. The technological sequence of data processing is built, which consists of solving certain conceptual problems, representing intermediate and final solutions.

Вступ. Жодне рішення не приймається без оброблення певної інформації. Чим більше обсяг наявної інформації й чим менш залежні її джерела, тим краще рішення.

Однак, велика кількість джерел характеризується різноманітністю форматів даних, які зберігаються в їх інформаційних ресурсах.

Особливості виникають при використанні інформаційних ресурсів, які містять природномовні тексти, які відображаються у неструктурованому чи слабо структурованому вигляді.

Виникає проблема – як швидко, а головне з найменшими затратами, використати недовідні дані з різноманітних інформаційних ресурсів такого роду.

Вирішення цієї проблеми можливо за рахунок використання певних процесів, які носять трансдисциплінарний характер при оброблення інформації для підготовки рішення [1]. Іншими словами створення визначеної технологічної послідовності обробки даних.

Викладення матеріалу дослідження. Дані з джерел неструктурованої або слабо структурованої інформації використовуються за допомогою відповідної технологічної послідовності обробки даних, яка складається з вирішення певних концептуальних задач, що представляють проміжні і кінцеве рішення. До них віднесемо наступні категорії, що визначаються як метазадачі [2]:

задача структуризації – проведення індексації текстового масиву та виділення його змістовної частини, яка формується відповідно до визначених категорій;

задача синтезу – формулювання нового концепту онтології та/або твердження в порядку розгляду від проблеми до структури; формулюється у вигляді правил виводу;

задача вибору – формування непорожньої множини концептів онтології

задачі на основі спеціально відібраної множини властивостей, що використовуються як певні критерії для формулювання істинних тверджень про стан її вирішення.

На основі вирішення вказаних задач можна визначити когнітивні сервіси (таблиця 1), які забезпечують певні процеси геопросторового аналізу та мають трансдисциплінарний характер [2-4].

Таблиця 1.

<i>Процеси геопросторового аналізу</i>	<i>Когнітивні сервіси</i>
Визначення потенційних джерел геопросторових даних та пов'язаної з ними інформації	Структуризація вхідної текстової інформації Індексне маркування інформаційних масивів Тематична класифікація інформаційних масивів та документів Автоматичне формування динамічних тематичних класифікаторів, каталогів та реєстрів інформаційних ресурсів Агреговане представлення інформаційних ресурсів Редагування таксономій
Пошук потрібних геопросторових даних та пов'язаної з ними інформації та створення формалізованого масиву несистематизованих даних	Внесення інформаційних масивів та документів у інформаційне середовище системи ТІЗ ГПА Індексне маркування інформаційних масивів Структуризація вхідної текстової інформації -таксономізація Редагування таксономій Збір тематичної інформації з визначених експертами-аналітиками інформаційних джерел
Структуризація інформаційного середовища та створення форматів його відображення.	Структуризація вхідної текстової інформації Таксономічне відображення структури інформаційних масивів Редагування таксономій Виявлення оптимальних закономірностей з різнотипних даних
Формування аналітичного середовища експерта-аналітика	Генерація онтологічних мережецентричних площадок користувачів Структуризація вхідної текстової інформації Таксономічне відображення структури інформаційних масивів Редагування таксономій
Синтез даних та моделювання ситуації.	Формування інтерактивних документів Структуризація вхідної текстової інформації Таксономічне відображення структури інформаційних масивів Редагування таксономій
Представлення та доведення до експертного середовища геопросторових даних і пов'язаної з ними інформації.	Структуризація вхідної текстової інформації Таксономічне відображення структури інформаційних масивів Ранжування альтернатив Раціональний вибір Прогнозне оцінювання Проведення багатокритеріального порівняльного аналізу Редагування таксономій

Процеси геопросторового аналізу	Когнітивні сервіси
Загальна оцінка ситуації, визначення причин її виникнення та вибір найбільш правильного варіанту рішення	Структуризація вхідної текстової інформації Таксономічне відображення структури інформаційних масивів Підтримка прийняття рішень у процесах класифікації, діагностики та виявлення властивостей на основі отриманих закономірностей з використанням нечіткої логіки. Автоматичне виявлення оптимальних закономірностей з різнотипних даних та їх представлення у явній формі логікових виразів Реалізація спільної обробки як числових так і номінальних даних у задачах виявлення та використання логікових виразів Редагування таксономій

Зазначена технологічна послідовність виглядає наступним чином (рис. 1).

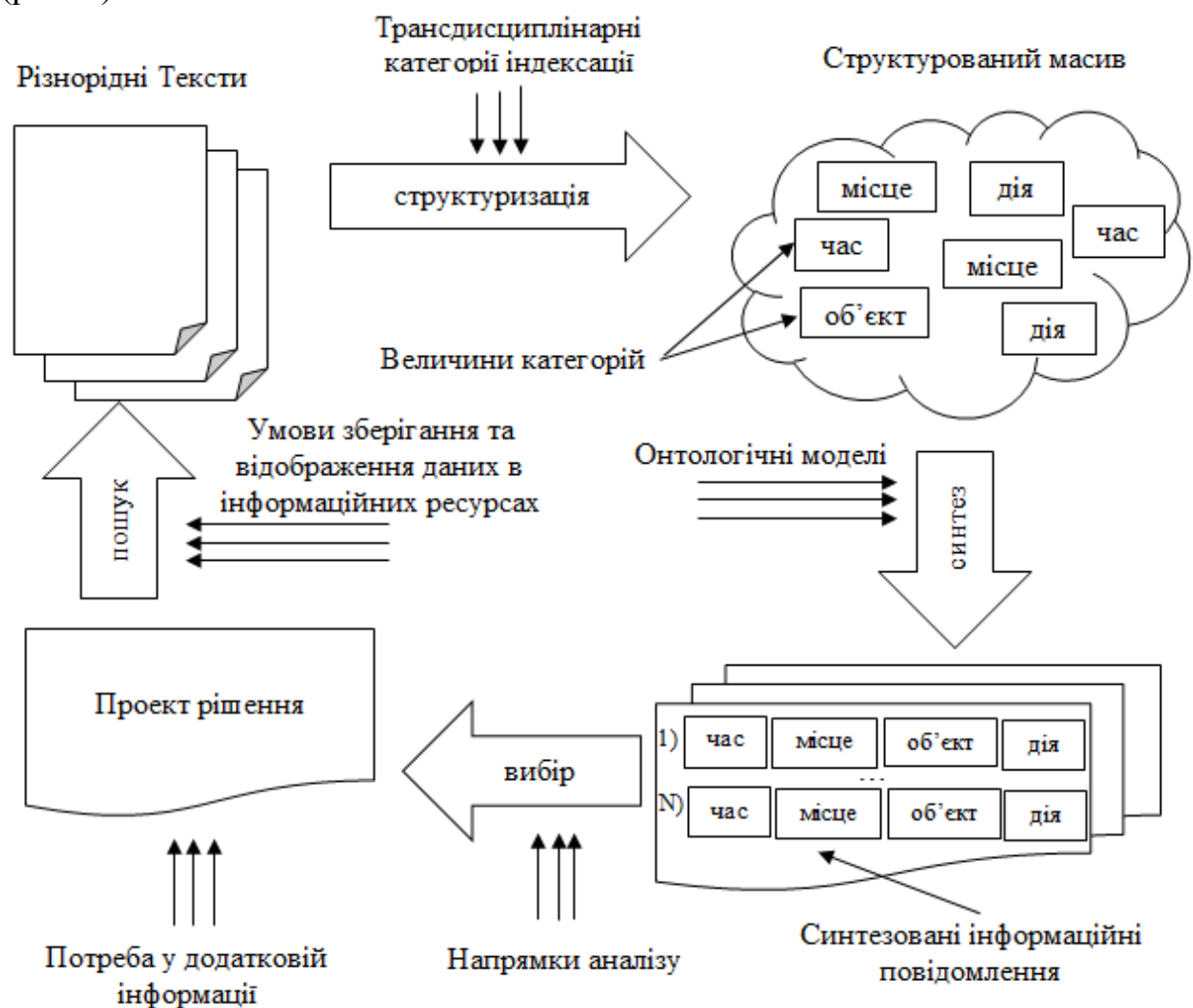


Рис. 1. Технологічна послідовність формування (організації) трансдисциплінарної інформаційної підтримки процесу геопросторового аналізу.

Вона складається з конкретних етапів, на кожному з яких здійснюються функція обробки інформації та обов'язково перехід на вищій більш якісний інформаційний рівень.

Отримавши різномірний неструктурований масив природномовних текстів здійснюється його структуризація. При структуризації використовується визначений набір категорій, за якими здійснюється індексація тексту. В результаті отримується структурований масив даних, в якому чітко визначені індекси кожної величини кожної категорії, за якими здійснювалась структуризація.

Наступним кроком вирішується задача синтезу. Певні контексти структурованого інформаційного масиву синтезуються відповідно до онтологічних моделей, в результаті чого формуються чіткі інформаційні повідомлення. Ці повідомлення є синтезованими та не мають зайвих даних. Вони представляють собою текстові масиви підвищеної інформаційної щільності.

Особливу роль відіграє задача вибору, кожен етап вирішення якої забезпечує коректне формулювання тверджень як послідовності описів станів вирішення прикладної задачі на основі критеріальної гармонізації їх властивостей.

Саме задача раціонального вибору та відповідна онтологічна система визначають інваріантність використання категорій зазначених метазадач [1].

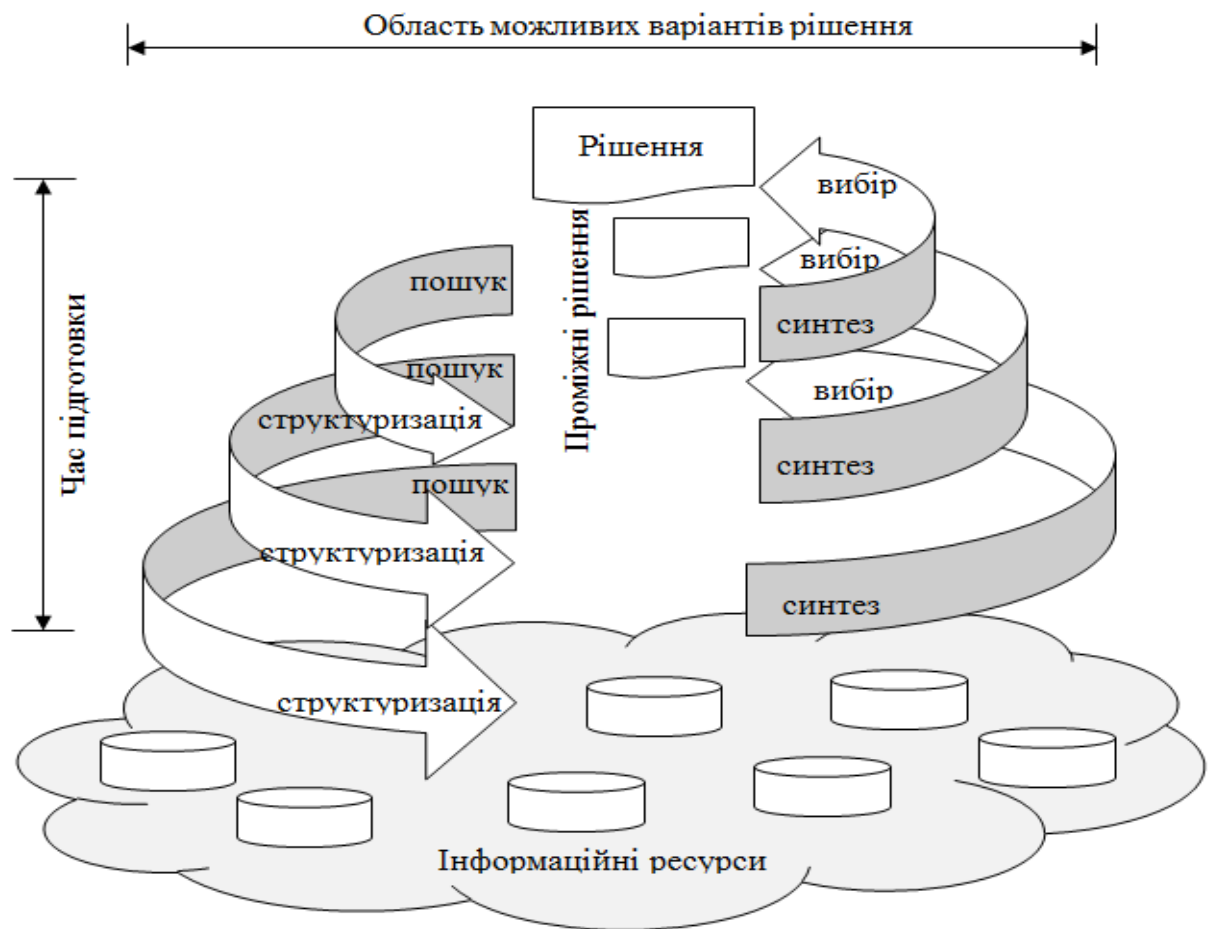


Рис. 2. Алгоритм формування достатні щільності інформаційної підтримки.

Враховуючи напрямки аналізу, за якими експерт-аналітик проводить дослідження, вирішується задача вибору. Із сформованих наборів інформаційних повідомлень обираються потрібні за тематикою або напрямком і додаються до аналітичного середовища та використовуються у процесі геопросторового аналізу і форматування проекту рішення [5-6].

По сутності це компоненти, які використовуються для обробки даних. Зазначені категорії задач присутні практично на кожному етапі процесу вирішення будь-якої прикладної задачі (рис. 2).

Комбінуючи та повторюючи ці задачі формується певний алгоритм обробки та підготовки інформації, необхідної для прийняття рішення експертом-аналітиком. У процесі роботи експерт-аналітик може прийняти декілька проміжних рішень, які будуть складовими остаточного рішення або певними його приближеннями. В випадку нестачі порідної інформація цикли повторіться доки приближення стане достатнім.

Висновки. Чім експерт-аналітик більше має часу на підготовку рішення, тим меншим буде область можливих варіантів рішень, а значить рішення буде більш раціональним. Однак це не завжди можливо, у зв'язки з різкими змінами ситуації або банальної відсутності достатньої кількості часу. Стабільність та певну достатність інформаційної підтримки процесу геопросторового аналізу забезпечує функціональні компоненти формування наборів когнітивних сервісів, які реалізуються на основі трансдисциплінарних онтологічних моделей геопросторових процесів, що аналізуються.

Література

1. Стрижак А. Е. Онтологические аспекты трансдисциплинарной интеграции информационных ресурсов / А. Е. Стрижак // Открытые информационные и компьютерные интегрированные технологии. – 2014. – № 65. – С. 211-223.
2. Стрижак О. Є. Трансдисциплінарна інтеграція інформаційних ресурсів : автореф. дис. д-ра техн. наук : 05.13.06 / Стрижак Олександр Євгенійович ; Нац. акад. наук України, Ін-т телекомунікацій і глобал. інформ. простору. – Київ, 2014. – 47 с.
3. Приходнюк В. В., Технологічні засоби трансдисциплінарного представлення геопросторової інформації [Текст]: автореф. дис. ... к-та техн. наук : 05.13.06 / Приходнюк В. В. ; Нац. акад. наук України, Ін-т телекомунікацій і глобал. інформ. простору. Київ, 2017. - 20 с.
4. Stryzhak O., Prychodniuk V., Podlipaiev V. (2019) Model of Transdisciplinary Representation of GEOspatial Information. In: Ilchenko M., Uryvsky L., Globa L. (eds) Advances in Information and Communication Technologies. UKRMICO 2018. Lecture Notes in Electrical Engineering, vol 560. Springer, Cham - p.34-72.
5. Подліпаєв В.О. Концепція побудови системи трансдисциплінарного інформаційного забезпечення геопросторового аналізу з компонентною архітектурою / В.О. Подліпаєв // “Системи управління, навігації та зв'язку” – Полтава.: ПНТУ ім. Ю. Кондратюка, 2019. – Вип. 3(55) С. 135-142.
6. Подліпаєв В.О. Базовий набір типових геоінформаційних ресурсів для здійснення геоінформаційної підтримки та ведення геопросторового аналізу / В.О. Подліпаєв // “Системи управління, навігації та зв'язку” – Полтава.: ПНТУ ім. Ю. Кондратюка, 2019. – Вип.. 2 (54). с. 12-37.

ЗАХИСТ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ШЛЯХОМ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

Гуменюк І.В., Сметанін К.В., Некрилов О.В.

Житомирський військовий інститут імені С.П. Корольова, Україна

E-mail: ig_gum@ukr.net

Protection against unauthorized access to information and telecommunications systems by biometric identification of users

The article proposes a method of blocking access to information and telecommunication systems, which is based on the algorithm of biometric identification/authentication by face geometry. It is shown that the application of the proposed method allows you to quickly identify the facts of unauthorized access by insider users of information and telecommunications systems and timely prevent information leaks.

Останні події, які спостерігаються на світовій арені, супроводжуються процесом перерозподілу зон впливу у технологічному та економічному просторі, розвитком інформаційних технологій (ІТ), які породжують нові способи отримання інформації. У зв'язку з цим, забезпечення захисту секретної інформації є актуальним питанням та вимагає від держав, незалежно від їх розвитку, постійного зміцнення національної безпеки, а також спроможності протидіяти загрозам і мінімізувати ризики реального витоку важливих відомостей та даних. При цьому важливо враховувати ефективність роботи автоматизованих підсистем управління доступом та захисту даних для забезпечення безпеки певної системи інформаційної інфраструктури, у тому числі інформаційно-телекомунікаційних систем (ІТС) [1].

Виходячи з даних передумов, сформульовано **мету** даної роботи, яка полягає у розробленні методу біометричної ідентифікації/аутентифікації і його застосуванні при вирішенні завдань блокування доступу до ІТС інсайдер-користувачами.

На даний момент розвитку ІТ паролі, які базуються на унікальній персональній інформації, та атрибутивні методи ідентифікації втрачають свою актуальність. Важливою проблемою цих методів є відсутність функціоналу для виявлення підміни авторизованого “легітимного” користувача. Порівняно з цими методами, біометричні характеристики користувача, як спосіб аутентифікації, можуть гарантувати підвищений рівень безпеки, враховуючи невід’ємність біометричних даних конкретної особи [2].

Розроблюваний метод включає такі кроки:

Крок 1. Виявлення та локалізація геометрії обличчя. У даній роботі використано алгоритм Віоли-Джонса. Обраний метод є кращим рішенням, порівняно з іншими алгоритмами, за критеріями ефективності та оперативності розпізнавання обличчя [3].

У загальному вигляді алгоритм здійснює пошук обличчя та її контури (геометрію) за допомогою сканування вікна. Відеозображення, на якому здійснюється пошук об'єкта, подається у вигляді двовимірної матриці розмірністю (x, y) , кожен піксель якої приймає значення для однотонного зображення $[0; 255]$ та для кольорового зображення формату RGB – $[0; 255^3]$.

Крок 2. Нормалізація зображення за масштабом, яскравістю тощо.

Крок 3. Обчислення набору базових ознак (характеристик) зображення.

Ознаки (примітиви) Хаара – це відображення f :

$$\chi \Rightarrow D_f \quad (1)$$

де D_f – множина допустимих значень ознаки.

За умови, що ознака $f_1, \dots, f_n$ визначена, вираз (1) прийме вигляд $\chi \Rightarrow \{f_1, \dots, f_n\}$, який називається ознакою опису об'єкта.

У процесі пошуку обчислювати всі ознаки Хаара практично не можливо, відповідно класифікатор повинен враховувати лише певну підмножину важливих ознак. Таким чином, для досягнення ефективності функціонування алгоритму та надійної роботи необхідно проводити інтелектуальне навчання класифікатора.

Крок 4. Порівняння обчислених ознак з еталонними.

Загальний алгоритм методу наведено на рис. 1.

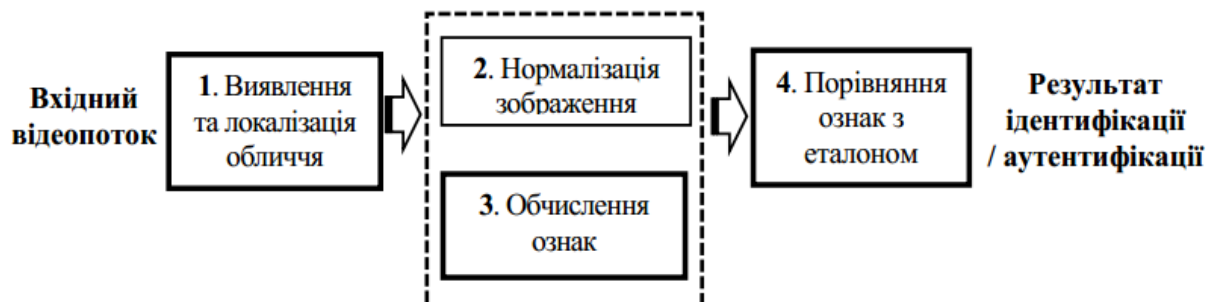


Рис. 1. Алгоритм блокування доступу інсайдер-користувачами до ІТС.

Верифікацію запропонованого методу проведено з використанням розробленого авторами спеціалізованого програмного забезпечення [4] на відеозображеннях, отриманих за допомогою відеокамери Infinity SR-DN530SD з роздільною здатністю відеопотоку HDTV 720p.

Умови проведення верифікації:

- до бази даних занесено 4 записи шаблонних користувачів ІТС (кожен запис містить до 30 зображень, прізвище, ім'я, унікальний номер тощо);
- природня (достатня та недостатня) освітленість приміщення – 100 – 400 люкс;
- мінімальна відстань між засобом відеоспостереження та об'єктом ідентифікації складає 0.5 м, максимальна – 2.5;
- кількість експериментів дослідження – 200;
- тестовими користувачами обрано одного з авторів наукової роботи (його дані занесені до БД) та двох інших користувачів, один з яких авторизований;

- одиночна (персональна) та групова ідентифікація.
Результати верифікації наведено на рис. 2–3.



Рис.2. Персональна ідентифікації при достатній освітленості:
а) відстань 0.5 (м); б) відстань 2 (м).



Рис. 3. Групова ідентифікація при достатній освітленості:
а) відстань 0.5 (м); б) відстань 2 (м).

Особливість методу інтелектуальної біометричної ідентифікації/аутентифікації користувачів ІТС полягає у можливості його реалізації у мобільних додатках, що особливо актуально в умовах інформатизації сьогодення. Практичне значення одержаних результатів полягає в можливості: впровадження методу в сучасні системи контролю та пропускового режиму ОІД; інтеграції програмного забезпечення в системи аутентифікації засобів обчислювальної техніки, у тому числі ПЕОМ; блокування доступу до інформації та засобів її обробки для несанкціонованих інсайдер-користувачів тощо.

Література

1. Гуменюк І. В., Басараба М. С., Некрилов О. В. Біометрична ідентифікація у кіберпросторі на основі розпізнавання обличчя // Проблеми теорії та практики інформаційного протистояння в умовах ведення гібридних війн: тези доповідей наук.-практ. конф. 24 – 25 жовтня 2019 р. Житомир : ЖВІ, 2019. С. 205–207.
2. Нечипоренко О. В., Корпань Я. В. Біометрична ідентифікація і автентифікація особи за геометрією обличчя // Вісник Хмельницького національного університету. Технічні науки. № 4, 2016. С. 133–138.
3. Немкова О. А. Біометрична ідентифікація у кіберпросторі // Системи обробки інформації. Випуск 7 (132), 2015. С. 118–121.
4. “Спеціалізоване програмне забезпечення біометричної ідентифікації/аутентифікації користувачів інформаційно-телекомунікаційних систем на основі геометрії обличчя”, Заявка про реєстрацію авторського права на твір № АПС 95-19. Дата затвердження заявки 28.10.2019.

**АЛГОРИТМ ВИЗНАЧЕННЯ ПАРАМЕТРІВ
РУХУ КВАДРОКОПТЕРІВ У МЕРЕЖАХ FANET**

Якорнов Є.А., Цуканов О.Ф.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: cukanov-o@ukr.net

An algorithm for determining quadcopter motion parameters in FANET networks

A stable algorithm for estimating the motion parameters of maneuvering quadcopters as elements of the FANET wireless sensor network is proposed based on the Kalman filter and the least squares method.

В роботі [1] була розглянута задача оцінювання параметрів руху безпілотних летальних апаратів (БПЛА), як елементів літаючих сенсорних мереж FANET. Враховуючи те, що останнім часом БПЛА на базі квадрокоптерів (КК) знаходять все більш широке застосування, виникає задача оцінки параметрів траєкторії їх руху, в тому числі і для мереж FANET.

Відмінністю КК від звичайного БПЛА є в управлінні траєкторією руху. Як показано в [1] управління БПЛА здійснюється шляхом зміни вектору швидкості, кутів нахилу траєкторії, ристання та тангажу. Математична модель руху в задачі оцінювання надається у вигляді поліномі третього ступеня. Такий підхід не може бути застосований під час рішення задачі оцінювання параметрів руху КК, оскільки він має в своєму складі чотири гвинта [2] і управління рухом а саме: швидкістю, напрямом та висотою здійснюється шляхом зміни швидкості обертання кожного з гвинтів.

Тому математична модель руху КК набагато складніше ніж звичайного БПЛА, оскільки траєкторія його руху може змінюватись як завгодно, а рух може розглядатися як "політ з постійним маневром".

Використовуючи методологію роботи [1] створимо модель руху КК, в якій інформація про параметри руху складається також зі вектору стану (ВС) в даний момент часу, якої має вигляд $X_{in}^T = [x_{in}, y_{in}, z_{in}, \dot{x}_{in}, \dot{y}_{in}, \dot{z}_{in}]$, а про помилки - у вигляді кореляційної матриці помилок (КМП) $\widehat{K}_{in}$. Тоді задача оцінювання ВС (параметрів руху) КК на підставі вхідної інформації про координати вектору вимірювань та КМП, яка є діагональною з елементами $\overline{\sigma x_i}, \overline{\sigma y_i}, \overline{\sigma z_i}$ зводиться до алгоритму, зображеному на рис.1.

Порівняємо даний алгоритм з наданим в [1], в якому для отримання високоточних оцінок параметрів руху БПЛА шляхом вимірювання координат пропонується використовувати як рекурентні методи на основі фільтру Калмана-Бьюсі, з більш простішою моделлю руху, так і оцінювання методом найменших квадратів (МНК) в "ковзному вікні" [3] складових швидкостей, а не прискорень для забезпечення стійкості.

Початковими умовами даного алгоритму оцінювання є також ВС

параметрів руху X_{in-1} і КМП K_{in-1} на $n-1$ кроці оцінювання, причому вектор вимірювань має вигляд $Y_{in}^T = [\hat{x}_{in}, \hat{y}_{in}, \hat{z}_{in}]$.



Рис. 1.

Екстрапольовані значення ВС X_{in}^e та КМП оцінки K_{in}^e можна представити у вигляді [4], на відмінно від [1], без урахування вектору управління

$$X_{in}^e = F_{in,n-1} X_{in-1}, \quad (1)$$

$$K_{in}^e = F_{in,n-1} K_{in-1} F_{in,n-1}^T + S_{in-1} \gamma, \quad (2)$$

де в (1) – (2) $F_{in,n-1}$ - матриця екстраполяції, S_{in-1} - КМП шуму моделі руху, який представляє собою середньоквадратичне відхилення оцінок прискорень за координатами x, y, z , γ – параметр стійкості (по результатам моделювання його оптимальне значення дорівнює 1.4).

Матричний коефіцієнт посилення [4] динамічного фільтра має вигляд

$$H_{in} = K_{in}^e (K_{in}^e + Q_{in})^{-1}. \quad (3)$$

де: Q_{in} - КМП вектору Y_{in} , на n - ому кроці вимірювань. Оцінки ВС $\hat{X}_{in}$ і КМП оцінювання $\hat{K}_{in}$ визначаються як

$$\hat{X}_{in} = X_{in} + H_{in} (Y_{in} - C_n X_{in}^e), \quad (4)$$

$$\hat{K}_{in} = K_{in}^e - K_{in}^e H_{in}, \quad (5)$$

Одночасно здійснюється оцінка значень вектору швидкості $\dot{x}_{in-1}, \dot{y}_{in-1}, \dot{z}_{in-1}$, за результатами апроксимації оцінювання координат в "ковзному вікні" шириною $\Delta t = [t_{k-1}, t_{k-m}]$. Модель руху маневрового БПЛА, описується алгебраїчним поліномом по кожній координаті ВС.

$$\tilde{X}_{n-1} = a_0 + a_1 t_{n-2} + a_2 t_{n-2}^2 \quad (6)$$

Далі за МНК визначається в "ковзному вікні" вектор коефіцієнтів по кожній з координат $Y = Y_{in-1}, Y_{in-2}, \dots, Y_{in-m}$

$$A = (N^T N)^{-1} N^T Y, \quad (7)$$

Знаходимо першу похідну від (6) (на відмінно від [1] де знаходимо одразу другу похідну) та отримуємо поліном по кожній з координат у вигляді

$$\tilde{V}_{n-1} = a_1 + 2a_2 t_{n-2} \quad (8)$$

де $\tilde{V}_{n-1} = [\hat{x}_{i,n-1}, \hat{y}_{i,n-1}, \hat{z}_{i,n-1}]$.

Вирази (1) - (8) являють собою запропонований стійкий алгоритм оцінювання. Завдання забезпечення стійкості алгоритму оцінювання параметрів руху КК, який постійно маневрує, вирішена шляхом обмеження знизу значень елементів матричного коефіцієнта посилення H_{in} за рахунок роботи фільтра Калмана (1)-(5) та уточнення елементів швидкості ВС. Розглянутий алгоритм уточнення моделі руху дозволяє забезпечити стійке оцінювання без блоку виявлення маневру при раптовій зміні траєкторії руху КК. Якщо БПЛА не робить маневр тоді всі складові вектору управління $\widehat{x_{i,n-1}}, \widehat{y_{i,n-1}}, \widehat{z_{i,n-1}}$ стануть постійними значеннями.

Результати імітаційного моделювання надані на рисунку 2, де показані залежності помилок по координатах та швидкостям під час зміни прискорення КК (середня помилка оцінки швидкості не перевищує 20 м/с).

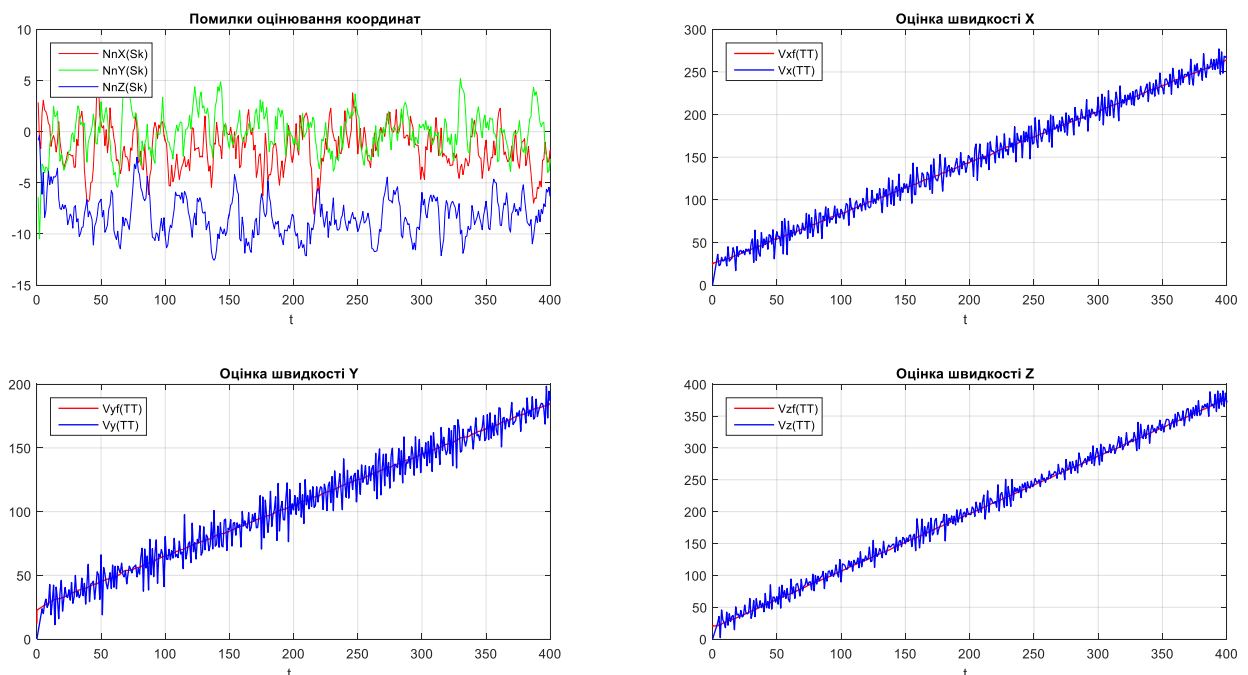


Рис. 2.

Таким чином, запропонований алгоритм дозволяє отримати стійкі оцінки параметрів руху КК із точністю близькою до оцінок звичайних БПЛА.

Література

1. Визначення параметрів руху маневруючих безпілотних літальних апаратів у мережах FANET.// Якорнов Є.А., Цуканов О.Ф. Матеріали XIII-ої Міжнародної науково-технічної конференції «Перспективи телекомунікацій» (ПТ-19) К.: НТУУ «КПІ ім. І.Сікорського», 2019, с. 285 – 287.
2. Лысенко А. И. Математическая постановка задачи оптимизации движения группы квадрокоптеров / А. И. Лысенко, С. Н. Чумаченко, Е. Н. Тачинина // Техническая механика. - 2016. - № 1. - С. 74-83.
3. Жук С.Я, Адаптивная фильтрация параметров движения маневрирующего объекта в прямоугольной системе координат. / Жук С.Я., Кожешкурт В.И., Юзefович В.В. //Регістрація, зберігання і обробка даних, - 2009, Т. 11, № 2, С. 12-24.
4. Grewal M.S. «Kalman Filtering». / Grewal M.S., Andrews A.P. //Theory and Practice Using MATLAB- Wiley, 2001.

УПРАВЛІННЯ МЕРЕЖЕЮ БПЛА ІЗ ВИКОРИСТАННЯМ SDN

Лисенко О. І., Валуйський С.В.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: samubf@gmail.com

UAV network control using SDN

The article describes main challenges and possible solutions for UAV network control system using SDN. It shows the main features required for UAV network and SDN capabilities to meet this requirements.

Мережі БПЛА є обмеженими в ресурсах зв'язку, вузли є непостійними, зв'язок переривчастий, і таким чином канали можуть бути порушеними. Це призводить до проблеми в плануванні та розподілі ресурсів. Різні мережі використовують різні протоколи маршрутизації і, отже, навіть вузли, які використовують ту саму технологію доступу (IEEE 802.11p чи IEEE 802.11s), не можуть працювати в іншій мережі через відмінності на вищих рівнях стеку протоколів. Зазначені проблеми можна було б вирішити за рахунок визначення стеку протоколів у програмному забезпеченні. Таким чином БПЛА можуть бути запрограмовані гнучко, щоб працювати в різних середовищах передачі даних. Однак це не єдина причина, чому програмне управління мережею є бажаним. Існує ряд інших вимог, що виникають у випадку таких мереж, як MANET, VANET та БПЛА мереж. Їм потрібно підтримувати мобільність вузлів та часті зміни топології. Вузли можуть вийти з ладу, наприклад, через розрядження акумулятора, і їх потрібно замінити на нові вузли. Канали є переривчастими і це також накладає певні труднощі на управління мережею. У цьому випадку доречним є застосування концепції SDN. SDN забезпечує спосіб програмного управління мережами, полегшуючи розгортання та управління новими додатками та послугами, а також дозволяє налаштовувати мережеві політики та продуктивність [1], [2].

Технологія SDN призначалася в основному для мереж із фіксованою інфраструктурою. Особливо широке застосування вона знайшла в центрах обробки даних (дата центрах), оскільки вважалося, що SDN підходить саме для мереж із централізованим управлінням, в той час як безпроводові ad hoc та mesh мережі були децентралізованими. Поділ на комутуючі пристрої та контролери також викликає певні проблеми із безпекою, балансом управління та гнучкістю. Однак через безумовні переваги, які надає технологія, у світі серед науковців і промисловості все більше зростає зацікавленість до застосування SDN в динамічних мобільних безпроводових мережах. У таких мережах, як VANET, використання SDN може допомогти у виборі маршруту та виборі каналу передачі даних. Це дозволить зменшити інтерференцію, покращити використання безпроводових ресурсів, включаючи канали та маршрутизацію в багатоланкових mesh мережах. Однак незважаючи на зростаючий інтерес, досі немає чіткого і всебічного розуміння

того, як переваги SDN можуть бути реалізованими для сценаріїв безінфраструктурних безпроводових мереж і як само концепція SDN повинна бути розширена відповідно до характеристик безпроводового та мобільного зв'язку [1].

Одним із часто використовуваних протоколів для впровадження SDN у безпроводових мережах є OpenFlow. Стверджується, що OpenFlow забезпечує істотні переваги для мобільних та безпроводових мереж. Він допомагає оптимізувати використання ресурсів у динамічному середовищі, забезпечує автоматизацію операцій, дозволяє кращий рівень управління та більш легке впровадження глобальних політик та нових сервісів. Протокол OpenFlow відокремлює функції комутації та контролю. Комутатори OpenFlow є програмованими та містять таблиці потоків та протокол взаємодії з контролерами [3].

Така мережа може бути сформована шляхом організації площини передачі даних, БПЛА комутаторів на основі OpenFlow, та площини централізованого управління на наземному контролері або розподіленого управління на мережі БПЛА. Елементи комутації (передачі даних) є простими комутаторами OpenFlow (не є IP-маршрутизаторами), що містять таблиці потоків, якими керує контролер по встановленим правилам. Таблиці потоків представляють собою набір критеріїв та відповідних дій, що визначають обробку, яка буде застосована до певного набору пакетів. В якості дій можуть виконуватись фільтрація, переадресація на певний порт, перезапис заголовка і т.і. На рис. 2а показано варіант реалізації площини централізованого управління на основі SDN в мережі БПЛА.

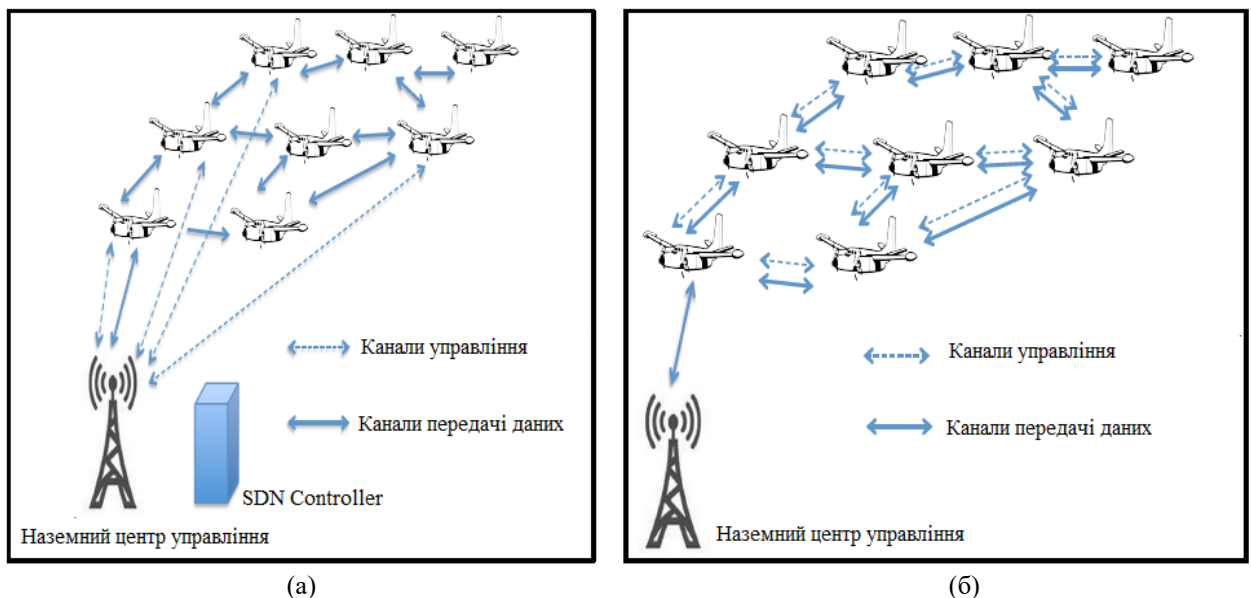


Рис.2. SDN з централізованим управлінням (а) та SDN з розподіленим управлінням (б).

Площина управління мережею SDN може бути централізованою, розподіленою або гібридною. Контролер має глобальний погляд на мережу і може ефективно маршрутизувати трафік. Він оновлює таблиці потоків комутаторів OpenFlow з відповідними критеріями та діями обробки [4]. У

централізованому режимі показано, що контролер, який визначає всі дії, що здійснюють безпроводові комутатори БПЛА, розміщений на землі. Але він також може бути повітряного базування. На малюнку 3б показано розподілене управління мережею SDN. У режимі розподіленого управління функції управління розподіляються між усіма БПЛА і кожен вузол контролює його поведінку. У гібридному режимі контролер делегує функції управління обробкою пакетів локальному агенту і таким чином між усіма елементами SDN передається трафік управління.

Дослідники з університету Карлстад (Швеція) продемонстрували можливість інтеграції OpenFlow з безпроводовими mesh мережами KAUMesh в невеликих масштабах [5]. Автори [2] наводять порівняння маршрутизації VANET на основі SDN з іншими традиційними протоколами маршрутизації MANET/VANET, включаючи GPSR, OLSR, AODV та DSDV. Вони зауважують, що маршрутизація на основі SDN перевершує інші традиційні ad hoc протоколи маршрутизації з точки зору коефіцієнта доставки пакетів для різних швидкостей. Головною причиною цього є сукупні знання, які має контролер SDN. У [6] автори узагальнюють сучасну ситуацію, кажучи, що SDN пропонує розширену конфігурацію, покращену продуктивність та заохочує інновації, але вона все ще знаходиться в зародковому стані, і багато фундаментальних питань все ще залишаються не повністю вирішеними. Можливості SDN для виконання різних вимог mesh мережі на основі БПЛА наведені в таблиці 1.

Таблиця 1. Потреби мережі БПЛА та можливості SDN.

Потреби мережі БПЛА	Можливості SDN
Підтримка мобільності вузлів	Реконфігурація за допомогою механізму оркестрації
Гнучкі стратегії комутації та маршрутизації	Гнучке визначення правил маршрутизації на основі заголовка або корисного навантаження пакету
Ненадійні безпроводові канали	Інтелектуальний вибір маршрутів та каналів
«Озеленення» мережі	Підтримує вимикання пристроїв, коли вони не використовуються. Підтримує агрегацію даних у мережі
Зменшення інтерференції	Можливе за рахунок вибору маршруту / каналу

Література

1. M. Mendonca, B. N. Astuto, K. Obraczka and T. Turletti, "Software Defined Networking for Heterogeneous Networks," IEEE MMTC ELetters, 2013, vol. 8, no. 3, pp. 36–39.
2. I. Ku et al., "Towards Software-Defined VANET: Architecture and Services," 13th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET), 2014, pp. 103–110.
3. N. McKeown et al., "OpenFlow: enabling innovation in campus networks," ACM SIGCOMM Computer Communication Review, 2008, vol. 38, no. 2.
4. A. Detti, C. Pisa, S. Salsano, N. Blefari-Melazzi, "Wireless Mesh Software Defined Networks (wmSDN)," IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Oct 2013, pp. 89–95.
5. P. Dely, A. Kassler, N. Bayer, "Openflow for wireless mesh networks," Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN), July–Aug 2011, pp. 1–6.
6. W. Xia, Y. Wen, C. H. Foh, D. Niyato and H. Xie, "A Survey on Software-Defined Networking," IEEE Communications Surveys & Tutorials, 2014.

ATTENUATION POLES IN BAND-PASS FILTERS WITH EVEN END ODD MODES

Ilchenko M., Zhivkov A., Akopian P., Galickiy I., Sobko T.

National Technical University of Ukraine “

Igor Sikorsky Kyiv Polytechnic Institute ”

Institute of Telecommunication systems

E-mail: ilyagal26@ukr.net

Полюса затухания в полосовых фильтрах с четными и нечетными модами

В докладе рассмотрены теоретические и экспериментальные характеристики полосового фильтра с полюсами затухания, образованного короткозамкнутым посередине полуволновым резонатором. Моделирование проведено с помощью программных продуктов Microwave Office и LabVIEW. Совпадение теоретических и экспериментальных результатов исследований свидетельствует об адекватности и эффективности выбранных моделей.

The report reviews the theoretical and experimental characteristics of a band-pass filter with attenuation poles formed by a half-wave resonator short-circuited in the middle. The simulation was carried out using the software products Microwave Office and LabVIEW. The matching of theoretical and experimental research results indicates the adequacy and effectiveness of the selected models.

A photograph of a microstrip filter, consisting of open circuit line and two parallel-connected resonators (short - “half-wave” and long - “wave”) is shown in Fig. 1. Such a filter design with a controlled bandwidth was considered in [1].

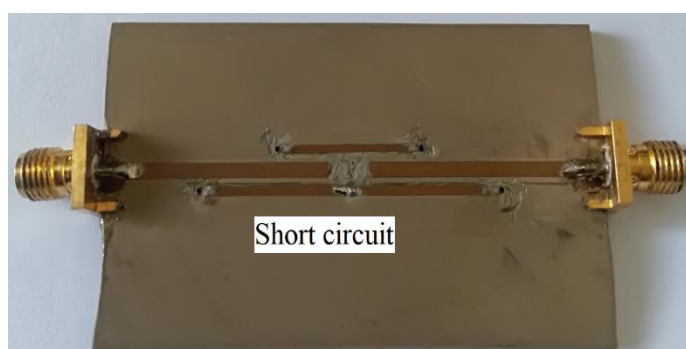


Fig. 1 Microstrip bandpass filter with two parallel resonators of different types.
The long resonator is short-circuited with a 2 mm loop in the middle.

It is known [2] that if a short-circuit (SC) loop is set in the middle of a strip resonator, its characteristic becomes similar to a two resonators filter. In the design under consideration, a dielectric substrate with $\epsilon = 9.8$ and a thickness of 2 mm was used; therefore, the SC at the operating frequencies of the resonator (of the

order of 1.5 GHz) is an inductance that affects the resonant frequencies of the even and odd oscillation modes differently [3].

Figure 2 shows the experimental (Fig. 2 a) and calculated in the Microwave Office software (Fig. 2 b) filter characteristics in the frequency range from 0.5 to 6 GHz. The presence of attenuation poles (p1 and p2 in Fig. 2 b), which are absent in the filter with a short-circuited middle resonator from [2], is noteworthy.

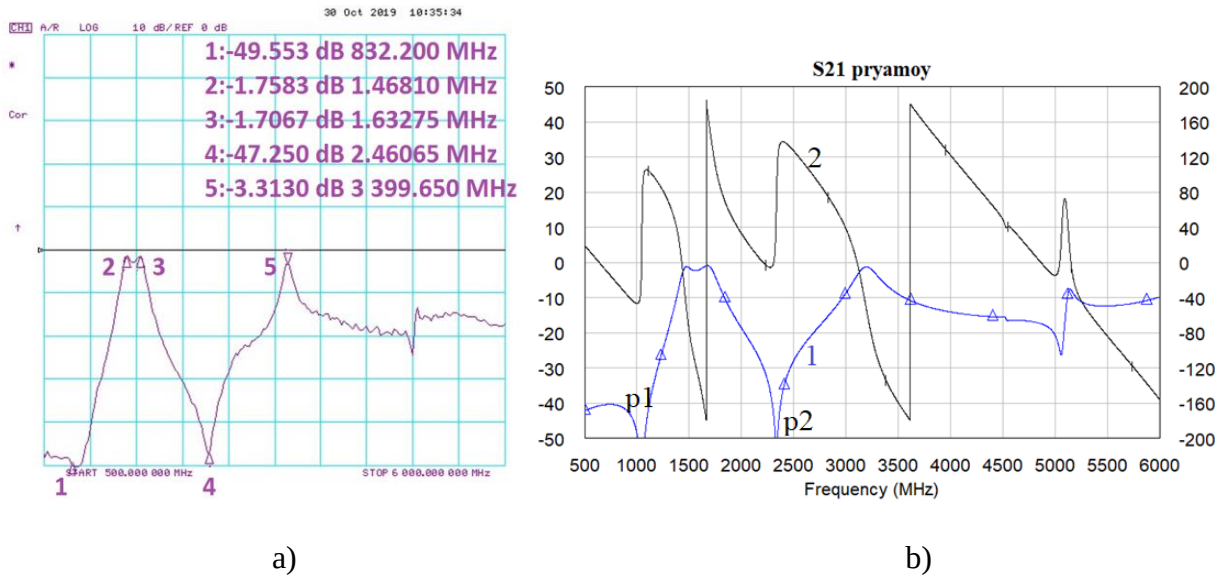


Fig. 2. Experimental a) and calculated b) characteristics of the strip filter Fig. 1.

Curve 1 in Fig. 2 b) is the amplitude of the transmission coefficient S_{21} ,
curve 2 is the phase of the transmission coefficient S_{21} .

The reason for the presence of attenuation poles is a short “half-wave” resonator with a resonant frequency of the order of 3.4 GHz. Indeed, since the resonators in this construction are not coupled, but are connected in parallel, there are at least two independent channels of energy transfer and a bridge equivalent circuit can be used to model the S-parameters of the filter [4].

An algorithm was developed for modeling bridge filters in the LabVIEW software, which allows us to clearly demonstrate the amplitude and frequency characteristics of both individual arms and the quadrupole as a whole on a graph. In fig. 3 a) are depicted the frequency dependences of $|S_{21}|$ of even (curve 1) and odd (curve 2) oscillations; curve 3 is the total characteristic of the quadrupole transfer coefficient, equivalent to the short-circuited in the middle “long” resonator. The frequencies on the characteristics on Fig. 3 are presented in relative units.

If now an another oscillation is added, simulating the short resonator in Fig. 1 (its resonant frequency corresponds $f_{rel}=200$ in fig. 3 b), then, as follows from fig. 3 b), the attenuation poles are formed at frequencies in the regions p1 and p2. The reason for the formation of the poles is the different “signs” of the reactances of the “loops” of oscillations 1, 2, and 3 (we can also speak of the inductive and

capacitive nature of the reactances and the “antiresonances” in the field of poles). An abrupt change in phase (curve 2 in Fig. 2. b) indicates a change in the sign of reactivity in the pole region (“antiresonance”).

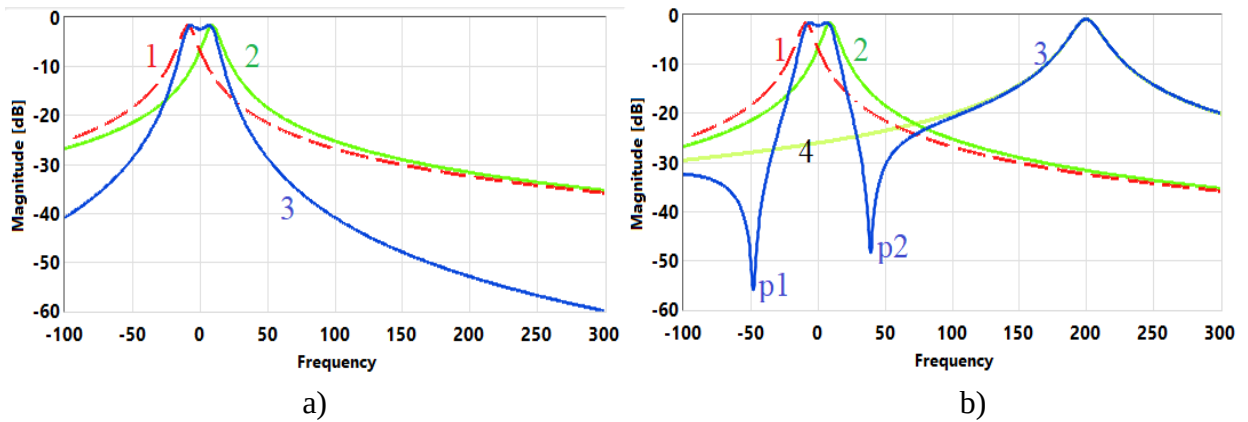


Fig. 3. Curves 1 and 2 in Fig. a) and b) are the characteristics of the in-phase and antiphase oscillations. Curve 3 is the characteristic of the filter as a whole.

Curve 4 - low-frequency slope of antiphase oscillation with a central frequency $f_{rel}=200$.

If the frequency of the second resonator is tuned, as was done, for example, in [1], then the position of the attenuation poles can be controlled.

References

1. USSR Inventor's Certificate 1518837.
2. Захаров А.В., Ильченко М.Е., Пинчук Л.С. Микроволновые резонаторы с двухмодовыми колебаниями.- Radioelectronics and communications systems, vol. 55, № 11 (2012), pp. 28-32.
3. Shou-Jia Sun*, Lei Lin, Bian Wu, Kun Deng, and Chang-Hong Liang. A novel quad-mode resonator and its application to dual-band bandpass filters progress in electromagnetics research letters, Vol. 43, 95–104, 2013.
4. M. E. Ilchenko, A. P. Zhivkov. Bridge Equivalent Circuits for Microwave Filters and Fano Resonance. in: Advances in Information and Communication Technologies. Springer, 2019, pp. 278-298.

ANOMALOUS DISPERSION AND GROUP DELAY OF METAMATERIAL CELLS

A. Zhivkov¹, R. Kamarali¹, M. Kopaniev², O. Krylach¹, I. Saychenko¹

¹*Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute,*

²*Kyiv College of Communication, Ukraine*

E-mail: zhivkovalex@gmail.com; theromarioagro@gmail.com

Аномальна дисперсія і груповий час затримки структур метаматеріалів

У даній роботі метаматеріальні структури розглядаються як два резонансних ланцюга (паралельний і послідовний), які з'єднані у вигляді паралельних і перехрещених входів 4- полюсного моста. Такий підхід дозволяє поширити деякі властивості мостових схем, що широко використовуються у метрології на метаматеріальні датчики. Наведено експериментальні та розрахункові характеристики метаматеріальних структур у мікрохвильовому діапазоні.

Bridge 4-poles for the first time began to be used in electrical engineering as precisely measuring chains [1,2]. In [2] it is noted that the Wheatstone bridge is used to accurately measure very low resistance values. At the beginning of the 20th century, bridge 4-poles began to be used as filters in high-frequency telephone communication networks [3]. In [4], the properties of a 4-pole bridge, which equivalent circuit is shown in Fig. 1, are examined in detail.

In particular, it is noted that due to the resonators finite Q factors (Q_1 and Q_2), the 4-pole may have characteristics with properties, that inherent to the Fano resonance. Figure 2 shows a microstrip bandstop filter photograph [5], where the dielectric sample is a plate 0.5 mm thick and the dielectric constant is $\epsilon = 10$. A change in the position of the plate relative to the resonator leads to a change in its resonant frequency. In this case, the filter transfer coefficient changes, as well as its shape and the maximum achievable attenuation [6].

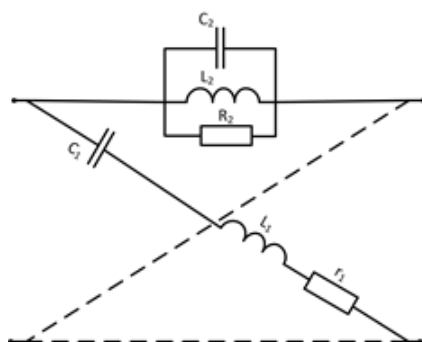


Figure 1. Bridge bandstop filter equivalent circuit.

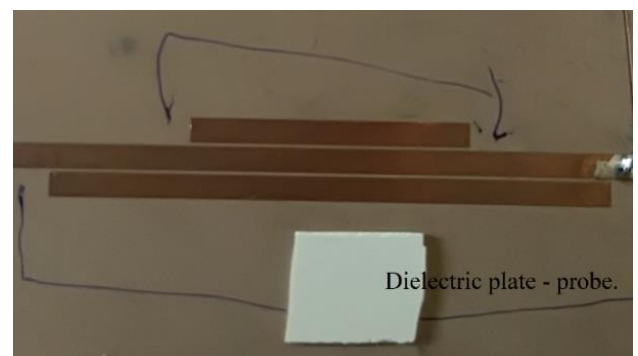
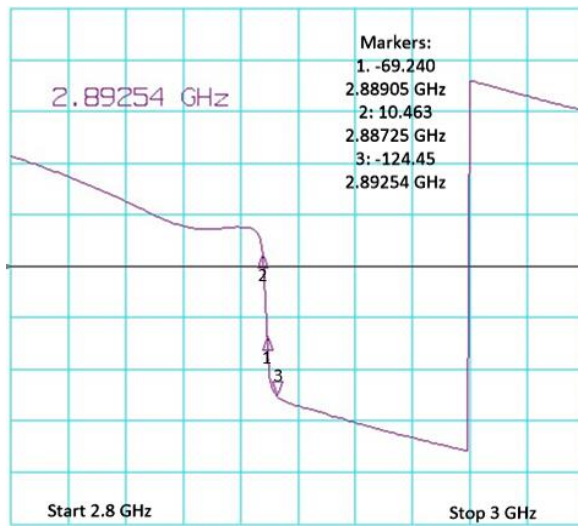
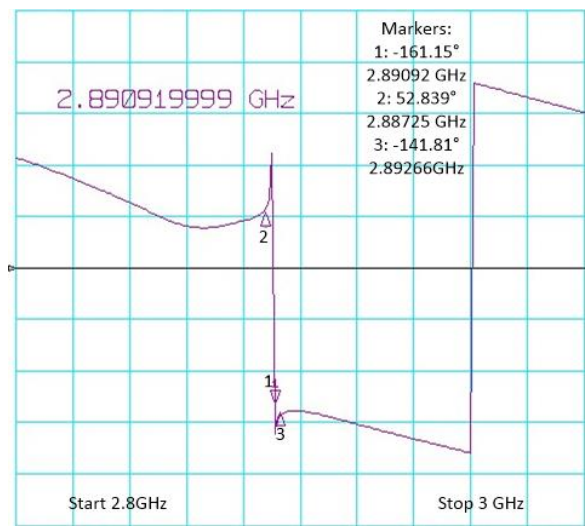


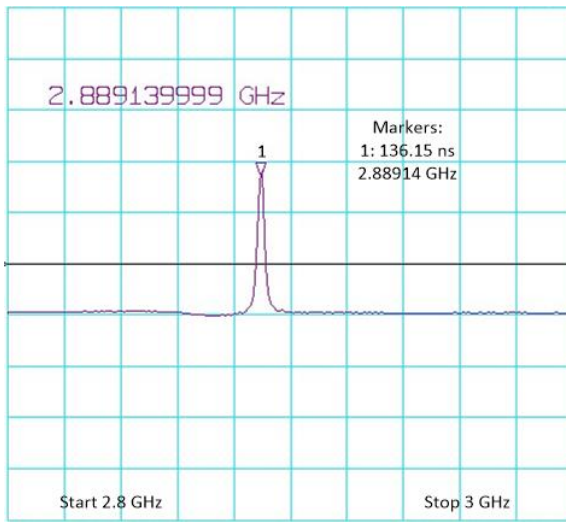
Figure 2. Microstrip bandstop filter with dielectric samples for frequency tuning.



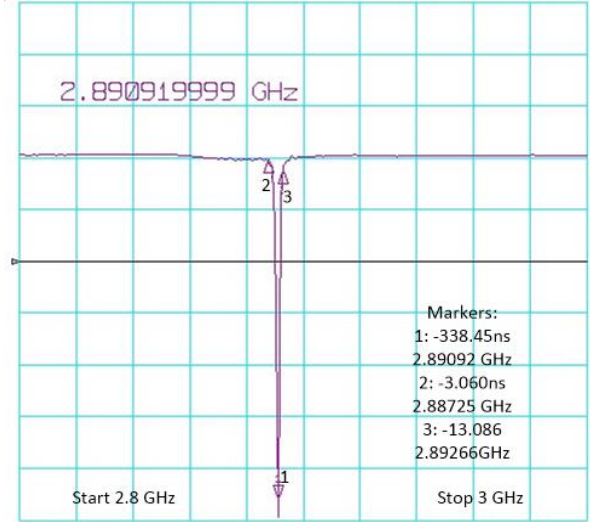
a)



b)



c)



d)

Figure 3. Phase characteristics (a, b) and their corresponding group delay time characteristics (c, d).

In articles, reports, and reviews that consider structures based on metamaterial cells as sensors [7–11], the amplitude characteristics of the transmission and reflection coefficients of such structures are mainly studied. At the same time, both calculated and experimental the metamaterial cells phase characteristics can also be used in the measurement process, which was demonstrated in [12]. Indeed, in the above-mentioned bridge structures measurement applications [1,2] the 4-pole balanced properties are used, that is why there is a possibility of achieving “0” in the measurement process”. The 4-pole transfer coefficient zero value is achieved at the Fano resonance [4], but it is difficult to accurately detect it because of the high sensor sensitivity in the resonance region. It is known that when “crossing the zero

value” the transmission coefficient changes sign, so that, its phase characteristic and phase derivative, which is the group delay time, change abruptly.

Conclusion: From the foregoing, it follows that in some cases, to increase the sensitivity of sensors based on metamaterials, it is necessary to analyze not only their amplitude, but also phase characteristics. It is also important to note that the large positive value of the group time delay does not mean that the causality principle is violated [13].

References

1. https://en.wikipedia.org/wiki/Bridge_circuit
2. <https://www.electronicshub.org/wheatstone-bridge/>
3. W. Mason. Physical Acoustic. Principles and Methods. V. 1. Methods and Devices. New York and London, Academic Press, 1964.
4. M. E. Ilchenko, A. P. Zhivkov. Bridge Equivalent Circuits for Microwave Filters and Fano Resonance. in: Advances in Information and Communication Technologies. Springer, 2019, pp. 278-298
5. USSR Inventor's Certificate 1529321.
6. M.E. Ilchenko and A.P. Zhivkov, “Areas of degeneration oscillations in metamaterial cells”, in 2017 Int. Conf. Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), pp. 1—4, 2017. doi: 10.1109/UkrMiCo.2017.8095389
7. Jordi Naqui *, Miguel Durán-Sindreu and Ferran Martín. Novel Sensors Based on the Symmetry Properties of Split Ring Resonators, Sensors 2011, 11, 7545-7553; doi:10.3390/s110807545
8. Jordi Naqui and Ferran Martín., Microwave Sensors Based on Symmetry Properties of Resonator-Loaded Transmission Line. Hindawi Publishing Corporation Journal of Sensors Volume 2015, Article ID 741853, 10 pages <http://dx.doi.org/10.1155/2015/741853>
9. La Spada L (2017) Metamaterials for Advanced Sensing Platforms. Res J Opt Photonics 1:1.
10. Ahmed Salim and Sungjoon Lim. Review of Recent Metamaterial Microfluidic Sensors. Sensors 2018, 18, 232; doi:10.3390/s18010232
11. F. Martín et al. Application of metamaterial concepts to sensors and chipless RFID. 2018 J. Phys.: Conf. Ser. 963 012012
12. Zhivkov A.P., Tsukanov O.F., Shevtsov K.O., Krylach O.F. “Phase frequency characteristics of metamaterial cells”. PT 2019, pp. 339-341
13. Bechhoefer J. Kramers-Kronig, Bode, and the meaning of zero, June 2011, American Journal of Physics 79(10), DOI: 10.1119/1.3614039

МЕТОД ВИЯВЛЕННЯ DOS АТАК В SDN МЕРЕЖАХ ІЗ ВИКОРИСТАННЯМ ЕНТРОПІЇ ШЕННОНА

Валуйський С.В., Єфименко О.С.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: o.yefymenko@gmail.com

Method of DoS attacks detecting in SDN networks using Shannon entropy

The article describes the technology of DoS attacks detecting using the method of calculating the entropy for traffic to destination IP addresses. Entropy is calculated by the Shannon formula, based on the analysis of the entropy value SDN controller redistributes the traffic between the scanners and changes the monitoring time intervals. This is how the DoS attacks are detected and further counteracted.

У статті описана технологія виявлення DoS-атак за допомогою методу обчислення ентропії трафіку до IP-адрес призначення. Ентропія обчислюється за формулою Шеннона, на основі аналізу значення ентропії контролер SDN перерозподіляє трафік між сканерами та змінює інтервали моніторингу часу. Таким чином здійснюється виявлення та протидія атакам DoS.

Централізоване управління є головною перевагою SDN, але у той же час і єдиною точкою відмови у разі виходу його із ладу. Однією з найпоширеніших причин, яка може вивести з ладу контролер SDN – це атаки DDoS, які можуть використовувати потенційні вразливості в контролері SDN [1], [2]. В даній статті пропонується метод побудови система виявлення вторгнень, що дозволить ефективно виявляти та протидіяти DdoS атакам в SDN мережі.

Запропонована система виявлення вторгнень складається з двох мережевих комутаторів (switches), основного SDN контролера та деякої кількості процесорів для обробки пакетів (сканерів), як показано на рисунку 1. Мережеві комутатори (S_1 та S_2) представляють собою вхідну та вихідну точки системи виявлення вторгнень. Мережевий комутатор S_1 відповідає за розподілення трафіку, який надходить до системи виявлення вторгнень із зовнішньої мережі, а S_2 збирає трафік від сканерів та направляє трафік до внутрішньої мережі. Коли трафік надходить до системи виявлення вторгнень, він пропускається через процесори для обробки пакетів ($P_1, P_2...P_n$).

Даний метод використовує тільки інформацію, що зберігається в адресному полі мережевого рівня PDU (protocol data unit моделі OSI), тож система не повинна бути пакетно-орієнтованою, також не потрібно проводити глибоке дослідження пакетів. Кожний сканер обробляє вхідний трафік та визначає атаку, використовуючи алгоритм, який базується на теоремі Шеннона. Якщо один з процесорів виявляє вище ніж нормальне навантаження по трафіку, правила розподілення трафіку на комутаторі S_1 налаштовуються для балансування кількості трафіку, спрямованого на кожен зі сканерів.

Механізм виявлення базується на значенні ентропії обчисленої для кінцевих адрес трафіку, який проходить через кожен сканер від комутатора S_1 . Ентропія розраховується за методом Шеннона, де p позначає ймовірність появи IP-адреси, як місця призначення пакету:

$$H = - \sum p * \log_2 p \quad (1)$$

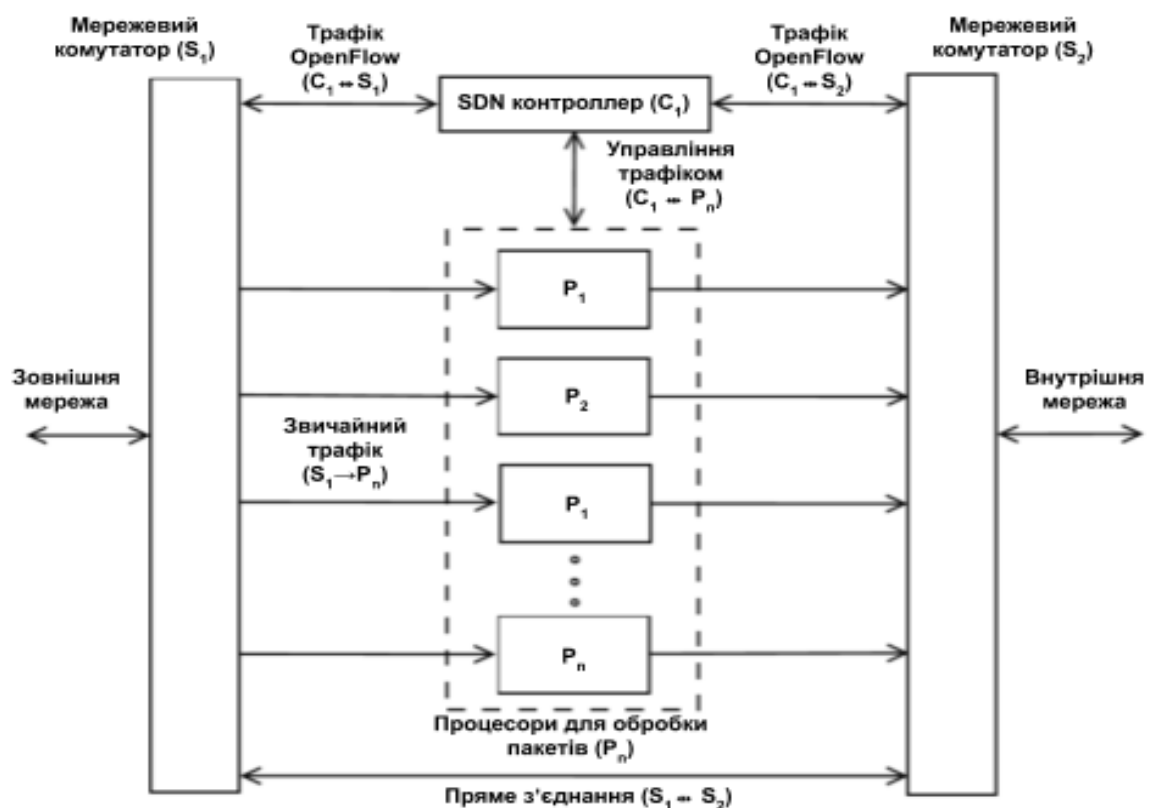


Рис.1. Архітектура системи виявлення вторгнень на базі SDN пристроїв (TIDS).

Основна ідея алгоритму полягає в тому, що зменшення значення ентропії для адрес призначення показує, що кількість трафіку, спрямованого на невелику кількість хостів, збільшилася і що зараз вона займає значну частину загального трафіку. Якщо зниження ентропії різке (воно відбувається за короткий проміжок часу), це може сигналізувати про те, що DoS атака розпочалась. Різниця в ентропії більш очевидна, коли трафік атаки займає більшу частку від загальної кількості трафіку (або коли інтенсивність фоновому трафіку менша порівняно з трактом атаки). Розподіляючи загальну кількість трафіку на декілька вузлів обробки, TIDS (Transparent Intrusion Detection System) зменшує кількість фоновому трафіку, який обробляється кожним процесором, тим самим підкреслюючи аномальний трафік та спрощує його виявлення. Крім того, процедура врівноваження тимчасово припиняється під час підозрілих мережових дій (тобто коли один з процесорів сигналізує про те, що в даний час можлива атака), щоб запобігти перерозподілу трафіку атаки між процесорами. Перерозподіл зменшив би інтенсивність трафіку атаки на процесор, який виявив підозрілу активність, тим самим збільшивши значення ентропії, що зменшило б шанси на успішне виявлення атаки. TIDS розділяє інтервал моніторингу на часові вікна (фрагменти), які містять статистику пакетів за цей часовий інтервал. Тривалість окремих фрагментів впливає на надійність та чутливість системи. Більш тривалі відрізки часу забезпечують стійкість до помилкових позитивних виявлень, які можуть з'являтися через короткі сплески мережового трафіку, тоді як більш короткі часові відрізки збільшують чутливість системи.

Література

1. P. Zanna, B. O'Neill, P. Radcliffe, S. Hosseini and S. Ul Hoque, 'Adaptive threat management through the integration of IDS into Software Defined Networks', 2014.
2. MM and K. Okamura, "Securing Distributed Control of Software Defined Networks," in International Journal of Computer Science & Network Security, vol. 13, no. 9, 2013.

ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННАЯ СИСТЕМА УПРАВЛЕНИЯ МИНИ-ТЕПЛИЦЕЙ С ИСПОЛЬЗОВАНИЕМ СЕРВИСНОГО РОБОТА

Нидченко И. А., Лысенко А. И.

Институт телекоммуникационных систем

КПИ им. Игоря Сикорского, Украина

E-mail: nidchenkoilya@gmail.com

Telecommunication-information system management of a mini-greenhouse using a service robot

Modern technologies have expanded the boundaries of human potential in the field of crop production, but the frequent cultivation and use of land leads to depletion of the soil and, as a result, to the forced use of fertilizers and chemicals to increase its fertility, but also the quality of vegetables and fruits is deteriorating. The way out of this situation is agricultural technology using mini-greenhouses in home. This is a high guarantee of the quality of cultivated plant products, but requires a lot of time and knowledge.

Современные технологии, несомненно, расширили границы возможностей человечества в сфере растениеводства, но частая культивация и использование земли приводит к истощению почвы, и, как следствие, к вынужденному использованию удобрений и химикатов для повышения ее плодородия. При этом их неправильное или избыточное применение отрицательно влияет на качество и полезность овощей и фруктов. Все большую популярность приобретают продукты, выращенные без применения или с минимальным применением удобрений и химикатов.

SALES OF ORGANIC PRODUCTS IN ITALIAN SUPERMARKETS (only pre-packed foods)

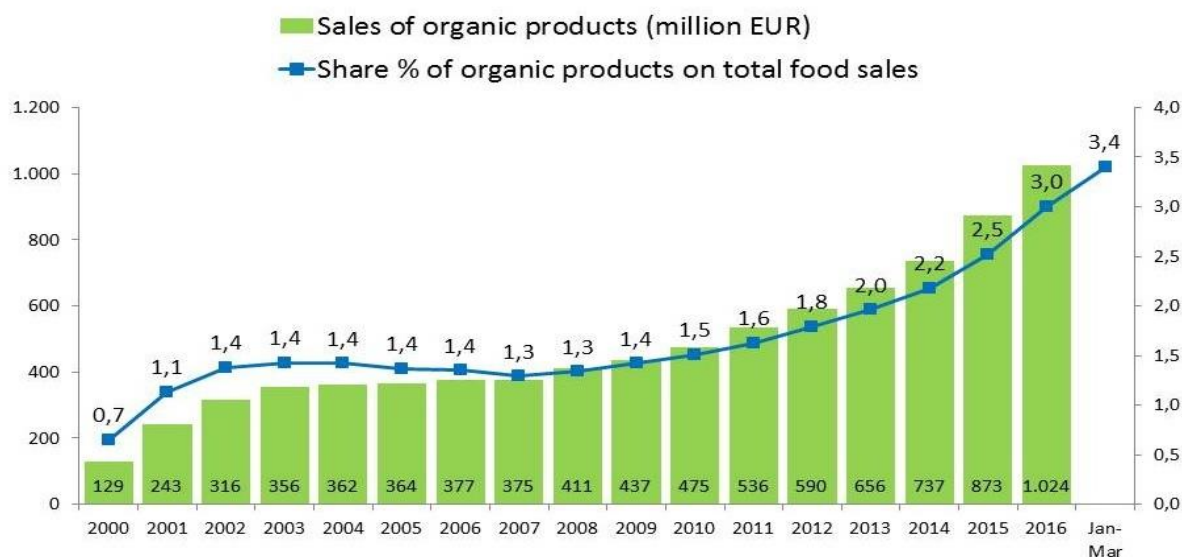


Рис. 1. Уровень продажи органической еды в Италии.

Выходом из этой ситуации являются агротехнологии с применением мини-теплиц в домашнем хозяйстве. Это высокая гарантия качества выращиваемых продуктов растительности, но требующая большого количества времени и знаний для правильного контроля производства.

Эту проблему можно решить, автоматизировав большую часть процессов при выращивании овощных и огородных культур с помощью информационно-телекоммуникационной системы управления мини-теплицей с использованием сервисного робота.

Данная система позволит производить удаленный мониторинг и диагностику параметров состояния почвы и воздуха, а также автоматизировать полив и освещение. Система состоит из микроконтроллера, датчиков влажности, температуры воздуха и почвы, освещенности, содержания углекислого газа, помпы с водой и фитоосвещением. Система имеет удаленный доступ к мониторингу и управлению показателями системы мини-теплицы через сервисного робота. Сервисный робот — это веб-приложение для сохранения с заданной периодичностью показателей, считанных сенсорами установленных в мини-теплице датчиков, составления графиков для анализа этих показателей, оповещения об их отклонениях от нормативных, а также о сбоях в работе системы из-за внешних факторов (например отключение электроэнергии).

Одной из важнейших составляющих информационно-телекоммуникационной системы управления мини-теплицей является микроконтроллер. При выборе микроконтроллера стоит обратить внимание на следующие параметры:

1. Разрешающая способность АЦП;
2. Наличие интерфейса I2C и SPI;
3. Частоту работы процессора;
4. Объем флеш-памяти;
5. Разрядность;
6. Дешевизна.

Самым популярным и подходящим ядром на данный момент является Cortex-M4. На базе этого ядра популярны 32-битные микроконтроллеры STM32 серии F – общего назначения. Они имеют бесплатные инструменты разработки, встроенный загрузчик (позволяет перепрограммировать внутреннюю флэш-память, используя некоторые коммуникационные периферийные устройства (USART, I²C)), низкую стоимость (32 цента за 32-битный контроллер, например, STM32G0), большой объем памяти (до 16 Мб).

Для удобства подключения и экономии проводов используются датчики с I²C шиной, которая может поддерживать до 100 устройств одновременно и требует лишь два коммуникационных провода. Данный протокол связи позволяет «общаться» с сенсорами на скоро 400кГц, чего более чем достаточно для нашей задачи.

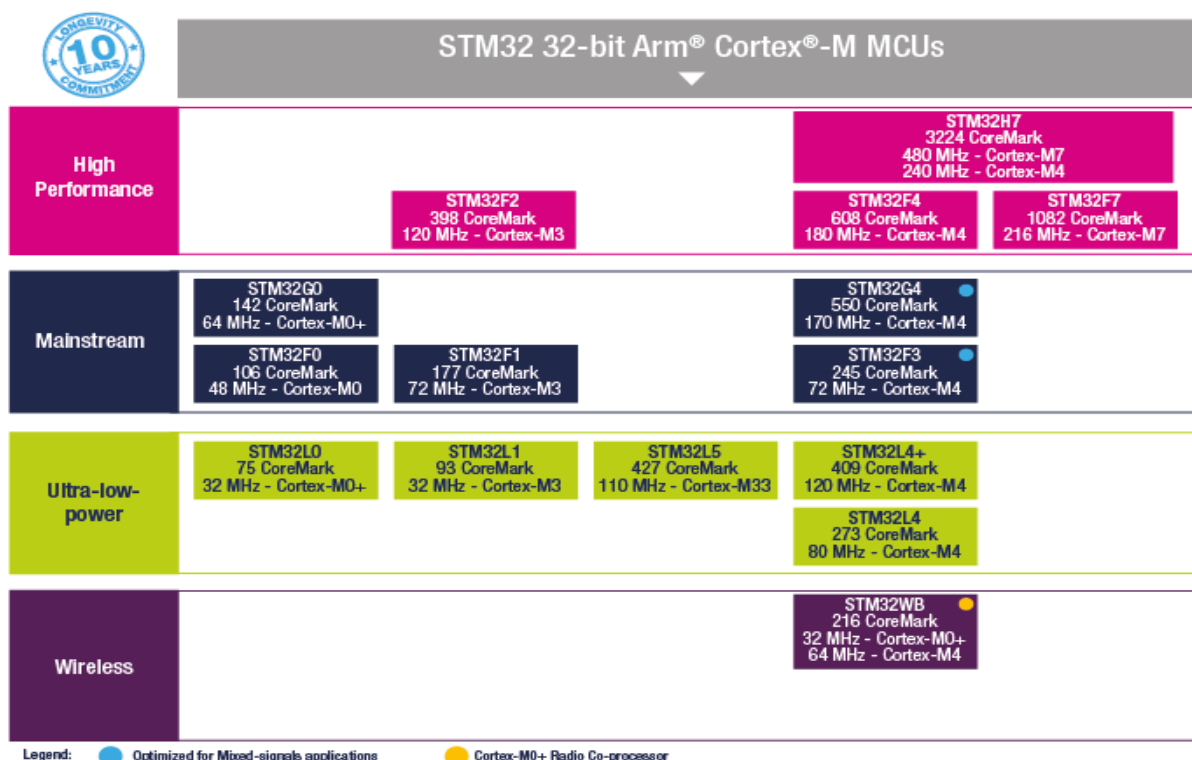


Рис. 2. Линейка микроконтроллеров STM32.

Основной проблемой ИС является допустимая длина шины в 10 метров. В больших масштабах теплицы рациональнее использовать радиосвязь. В условиях малого количества информации и желательно большой площади покрытия рекомендуется использовать протокол LoraWAN. Данный сетевой протокол обеспечит мобильность, безопасность и двустороннюю связь. Это усложнит разработку системы, но упростит монтаж и использование.

Применение информационно-телекоммуникационной системы управления мини-теплицей с использованием сервисного робота позволит наладить и оптимизировать процесс выращивания овощей в любом домохозяйстве, так как данная система может использоваться без наличия специального опыта, она достаточно проста в управлении и доступна, а веб-приложение имеет понятный интерфейс.

Литература

1. Carmine Noviello (2018), «Advantages of the STM32 Portfolio....», «The I²C Protocol», Mastering STM32, pp. 22-24, 427-428.
2. STM32 32-bit Arm Cortex MCUs family –
Site: <https://www.st.com/en/microcontrollers-microprocessors/stm32-32-bit-arm-cortex-mcus.html>

АНАЛІЗ СТАНУ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ LTE ПРИ ОРГАНІЗАЦІЇ ВИСОКОШВИДКІСНОГО АБОНЕНТСЬКОГО ДОСТУПУ

Явіся В.С.

*Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: yavisya@bigmir.net*

Analysis of the state of implementation of LTE technology in the organization of high-speed subscription access

To estimate the speeds that LTE technology can provide, it is necessary to consider the channel organization method, the given frequency range, the modulation type, the information code method, the use of MIMO technologies, the use of management resources. Theoretical speed limitation is 1 Gbit/s in descending direction (from base station to subscriber) and three to four times slower speed - from subscriber to base station. The analysis shows that the average access speed for mobile subscribers in the data channel is on average not more than 37.71 Mbit/s. Access speed in the uplink channel will be even lower than marked.

Відмінною рисою сучасних мереж безпроводового доступу є стрімке впровадження технології LTE (Long Term Evolution – довгострокова еволюція), яка забезпечує високошвидкісний мобільний доступ в Інтернет. Теоретичною межею швидкості є понад 1 Гбіт/с у спадяючому напрямку (від базової станції до абонента) і у три-чотири рази менша швидкість – у висхідному (від абонента до базової станції). Наприклад на сайті «Київстар» йдеться про швидкість завантаження даних до 700 Мбіт/с і передачі – до 90 Мбіт/с [1]. Якою ж є справжня швидкість? Ще у 2018 році фахівці «Vodafone Україна» і Nokia провели випробування стандарту LTE 2100 і LTE 1800 FDD. Тестування фрагмента мережі проходило протягом двох місяців на технічному майданчику в закритому приміщенні. Перевірялася взаємодія мереж UMTS і GSM з мережею LTE з підтримки функціонування базових сервісів в частині передачі даних, забезпечення голосового виклику і SMS, агрегація частот з спектрів 2100 і 1800 МГц. Під час тестування пікова швидкість отримання даних перевищила 173 Мбіт/с, а передачі даних – 48 Мбіт/с [2]. За останніми дослідженнями було зібрано 85 тестів швидкості від абонентів «Київстар», 62 – «Vodafone Україна» і 52 – Lifecell з усіх областей України. Лідером за швидкістю завантаження виявився Lifecell з середньою швидкістю в 37,71 Мбіт/с. А пальма першості по вивантаженню у «Київстар» – 16,41 Мбіт/с.

Для оцінки швидкостей, які може забезпечити технологія LTE у спадяючому й висхідному каналах, важливо брати до уваги кілька важливих параметрів: метод дуплексування каналів, наявний діапазон частот, вид модуляції піднесучих, метод завадостійкого кодування даних, використання технологій MIMO (Multiple Inputmultiple Output), витрати ресурсів на управління, тривалість циклічних префіксів та ін. [3].

Принципово новим розв'язком для радіо інтерфейсу LTE стало використання нових методів множинного доступу – OFDMA у спадаючому каналі (Orthogonal Frequency Division Multiple Access) і SC-FDMA (Single Carrier Frequency Division Multiple Access) – у висхідному. Важливо, що весь наявний спектр розбивається на ортогональні піднесучі по 15 кГц (у спадаючому каналі), кожна з яких, у свою чергу, модулюється певним видом модуляції (від QPSK до QAM256). Мінімальна смуга, що виділяється для одного абонента – 12 піднесучих. Очевидно, що використання багатопозиційних методів модуляції вимагає каналів з високим рівнем відношення сигнал/шум, погіршення ж радіо умов приведе до зниження порядку модуляції, а відповідно й швидкості передачі даних. Крім порядку модуляції важливо брати до уваги й схему завадостійкого кодування. Наприклад, кодування зі швидкістю 1/2 ще у два рази знижує швидкості передачі даних.

Найважливішою особливістю мереж LTE є масштабованість займаного ними частотного спектра від 1,4 до 20 МГц. Очевидно, що чим ширша смуга, тим більше будуть швидкості.

Мінімальною одиницею надання доступу одному користувачеві є ресурсний блок (їх кількість становить від 6 до 100 залежно від наявного спектру) – це 12 піднесучих у частотній області й один тайм-слот, або 7 OFDM-символів у часовій області тривалістю 0,5 мс. Піднесучі по краях спектра, як правило, використовуються в якості захисних інтервалів.

Немаловажним фактором при оцінці можливостей LTE є застосування технології МІМО. Існують кілька варіантів застосування МІМО: 2x2, 4x4 та навіть 8x8. Для збільшення абонентської ємності, при цьому з різних антен передається різна інформація. У цьому випадку використання МІМО приведе до збільшення швидкості передачі даних у спадаючому каналі відповідно у 2, 4 або 8 разів. Однак реалізація такої схеми зажадає додаткові частотно-часові ресурси для передачі опорних пілот-сигналів антен.

Інформація, передана на радіо інтерфейсі, ділиться на службову інформацію, яка транслюється по різних каналах управління, і на дані користувача каналу PDSCH (Physical Downlink Shared Channel). Оскільки більшість операторів, що запустили LTE, мають спарені смуги частот для висхідного й спадаючого потоків, то розглянемо особливості саме FDD-режиму, структуру його сигналу й співвідношення між службовими ресурсами та ресурсами користувача.

Для того щоб оцінити швидкості передачі даних у спадаючому каналі, спочатку оцінімо, скільки ресурсних елементів (або OFDM-символів) передається в часовому інтервалі, що дорівнює 1 мс, залежно від наявної смуги частот.

В одному субкадрі (два тайм-слоти) на одній піднесучій передається до 14 OFDM-символів. Таким чином, число OFDM-символів буде дорівнювати: $14 \cdot 12 = 168$ (12 – число, піднесучих у ресурсному блоці). Далі із загального числа символів, необхідно відняти число символів, виділених під канали управління. Коли використовується FDD-режим, 49 OFDM-символів

зайняті службовою інформацією – 29% частотно-часового ресурсу [4]. У такий спосіб усього $168-49=119$ символів використовуються для передачі даних користувача.

Інформаційні символи, що залишилися, необхідно помножити на кількість біт, які вони можуть містити. Число біт у символі буде визначатися способом модуляції піднесучих – 2, 4, 6 або 8 біт відповідно до алгоритму QAM.

Далі необхідно врахувати вплив завадостійкого кодування. Як правило половина від отриманого числа біт піде на надмірність.

Використання МІМО збільшує швидкість у кратне число раз. Це самі основні особливості, які необхідно враховувати при оцінці швидкості.

Виконавши подібні розрахунки, нескладно одержати швидкості передачі даних у спадаючому каналі.

Реальна швидкість доступу для мобільних абонентів у спадаючому каналі, з урахуванням складності технічної реалізації МІМО, при поганих умовах приймання (використовується QPSK та перешкодостійке кодування) і наданні користувачеві одного ресурсного блоку складе $119 \cdot 2 \cdot 2 \cdot 1000 = 119$ кбіт/с, а при максимальній смузі частот 20 МГц (до 100 ресурсних блоків) і ідеальних умовах приймання (використовується QAM256 без перешкодостійкого кодування) – до $119 \cdot 8 \cdot 100 \cdot 1000 = 95,2$ Мбіт/с. Швидкість доступу у висхідному каналі буде ще меншою від зазначених.

Для поліпшення ситуації, що склалася з доступом до мобільного інтернету, збільшення території покриття та прискорення будівництва 4G-мереж на території країни Кабінет Міністрів України схвалив рішення про перерозподіл радіочастот в діапазонах 800-900 МГц [5].

Таким чином, при застосуванні технології LTE, заявлена швидкість безпроводового доступу для користувачів може бути меншою, ніж та що очікується і яка заявлена постачальниками обладнання. Враховуючи вище зазначене, а також необхідність значних інвестицій на розгортання мережі LTE, постачальникам послуг варто здійснювати аналіз терміну окупності та можливих прибутків з урахуванням можливостей інших технологій безпроводового доступу.

Література

1. Тестирование Mind: какой скоростью 4G удивляют абонентов мобильные операторы URL: <https://mind.ua/ru/publications/20194703-testirovanie-mind-kakoj-skorostyu-4g-udivlyayut-abonentov-mobilnye-operatoru> (дата звернення: 10.03.2020).
2. 4G/LTE в Украине. Диапазон частот, зона покрытия, операторы, тарифы. URL: https://www.workmobiles.ru/tags/LTE_v_ukraine (дата звернення: 10.03.2020).
3. Явіся В.С., Вакуленко О.В. Оцінка швидкості передавання у мережах 4G // XI Науково-практична конференція «Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення. Застосування підрозділів, комплексів, засобів зв'язку та автоматизації в операції Об'єднаних сил». Доповіді та тези доповідей. – К.: ВІТІ. – 2018. – С. 238-239.
4. Дроздова В.Г., Белов М.А. Оценка пропускной способности сетей LTE. // Мобильные телекоммуникации. – 2012. – №5. – С. 20-22.
5. В Украине перераспределили частоты для 4G. URL: <https://deps.ua/novosti/novosti-rynka/item/68243.html> (дата звернення: 10.03.2020).

СПОСІБ ПІДВИЩЕННЯ ЯКОСТІ КАНАЛУ УПРАВЛІННЯ ДРОНАМИ

Явісія В.С., Лисенко О.І.

Інститут телекомунікаційних систем «КПІ ім. Ігоря Сікорського», Україна

E-mail: yavisya@bigmir.net

Method of improving the quality of drones management

Drones of small size with electric motor are widely used in various fields. It is necessary to ensure the quality of the control channel between the ground control center and the drones. It is suggested to use directional antennas on drones. Traditional ways to accomplish this task are evaluated in the light of limitations on weight, size and energy characteristics.

Сьогодні за допомогою мультикоптерних дронів малих розмірів з електродвигунами можна контролювати технічний стан об'єктів, їх безпеку та режими функціонування, дрони можна використовувати з метою аерофотознімання для картографування, угруповання дронів дозволяють підвищити показники телекомунікаційних мереж (живучість, пропускну здатність), вони можуть доставляти вантажі і т.п.

Як правило, будь-яке застосування дронів передбачає, що одержувана з їхньою допомогою інформація й безпосередньо сигнали управління дронами повинні передаватися в реальному часі, що вимагає забезпечити передачу великого обсягу даних при заданих смузї пропускання й імовірності бітової помилки.

Для підвищення пропускну здатності необхідно використовувати спектрально-ефективні методи модуляції, що змушує забезпечити більш високе відношення сигнал/шум (ВСШ) на вході приймача. При цьому висувуються жорсткі вимоги як по мінімізації розмірів приймально-передавального і антенно-фідерного встаткування, так і по споживаній ними потужності.

Для задоволення вимог по ваго-габаритним показникам і по пропускну здатності доцільним є вибір надвисоких частот (НВЧ), а саме, діапазону 2,4 ГГц, у якому залежно від поточного значення ВСШ можна використовувати модуляцію від BPSK до QAM256, які забезпечують високу спектральну ефективність [1].

Дрони як правило використовуються на відстанях до 10 км, тому обмежень, пов'язаних з «прямою видимістю» для них не існує, оскільки при висоті польоту 50 м і висоті наземного комплексу управління (НКУ) 1,5 м (за умови його знаходження в руках оператора), дальність прямої видимості, яка визначається формулою [2]:

$$D_{\text{км}} = 4,12(\sqrt{h_1} + \sqrt{h_2}),$$

де h_1, h_2 – висоти дрону й НКУ відповідно, складе більше 30 км.

У діапазоні 2,4 ГГц загасання сигналу на відстані 10 км досягає 120 дБ [1], тому необхідно передбачити заходи, що дозволяють забезпечити

необхідний енергетичний рівень переданого сигналу на такий відстані. Аналіз ринку малогабаритних приймально-передаючих пристроїв показує, що найпоширеніші приймачі із чутливістю порядку -90 дБ, і передавачі з посиленням близько 30 дБ, що дозволяє перекрити загасання в 120 дБ.

Однак, для забезпечення ймовірності помилки порядку 10^{-6} при використанні QAM32 на вході приймача необхідне ВСШ на рівні 18 дБ [2]. Враховуючи втрати у фідері приймача й передавача (усього близько 3 дБ), стає зрозумілим, що енергетика переданого сигналу повинна бути збільшена, як мінімум, на 21 дБ, а в реальних умовах поширення сигналу й впливу ненавмисних перешкод – на ще більшу величину. Розв'язати таке завдання можна шляхом використання спрямованих антен.

Для параболічної антени коефіцієнт підсилення розраховується за формулою [2]:

$$G = 10 \lg(k(\pi D / \lambda)^2 \cos \varphi) \quad (1)$$

де: G – коефіцієнт підсилення; k – ефективність або коефіцієнт використання поверхні антени (для більшості антен рівний приблизно $0,55$); D – діаметр дзеркала; λ – довжина хвилі; φ – кут приходу хвилі.

Відповідно до виразу (1) при діаметрі дзеркала $0,5$ м, точно спрямованій антені на дрон ($\varphi = 0$), у діапазоні $2,4$ ГГц коефіцієнт підсилення складе лише $19,4$ дБ. Подальше підвищення коефіцієнта підсилення може бути здійснене за рахунок збільшення діаметра дзеркала, що важко реалізувати для носимих НКУ. Зрозуміло, що рівень сигналу повинен бути підвищений «із запасом» приблизно на 5 дБ.

Завдання підвищення рівня сигналу може бути вирішене шляхом установки на борту дрона спрямованої антени.

Управління напрямком максимального посилення бортової антени може здійснюватися декількома способами [3]: установка антени на опорно-поворотному пристрої; використання багатоелементної антенної решітки з керованою діаграмою спрямованості; використання декількох антен, що перемикаються.

Реалізація першого способу дозволяє використовувати одну гостроспрямовану антену для безперервного спостереження за напрямком на НКУ. При установці антени на опорно-поворотному пристрої необхідне створення обертового переходу. Він може бути розміщений у різних місцях: перед антеною після підсилювача потужності; після передавача перед підсилювачем потужності й антеною; передавальний пристрій, підсилювач потужності й антена розміщуються на поворотному пристрої, через багатоканальний обертовий перехід передаються сигнали та живлення.

Загальними недоліками використання опорно-поворотного пристрою є:

- висока вартість обертового коаксіального НВЧ переходу;
- при розміщенні гостроспрямованої антени будь-якого типу на опорно-поворотному пристрої, більша частина поверхні поворотної платформи залишається невикористаною. Для підвищення ефективності використання

площі поворотної платформи необхідно розміщати на ній крім антени передавальне встаткування та підсилювач потужності;

- переміщення антени в горизонтальній площині приводить до переміщення центру ваги дрону, а отже до дестабілізації його просторового положення;

- значні витрати потужності на роботу електропривода.

При реалізації другого способу для створення антенної системи з керованою діаграмою спрямованості може бути використана кільцева антенна решітка. Завдяки кільцевій симетрії антенної решітки вдається одержати спрямовані діаграми, які мало змінюються при скануванні в межах 360° у площині решітки.

Однак, для одержання посилення кільцевою антенною решіткою необхідно збільшувати число елементів, що у зв'язку з ваго-габаритними обмеженнями неприйнятно для мультикоптерних дронів з електроприводом. Крім того, використання багатоеlementної антенної решітки ускладнюється необхідністю виготовлення складних і високовартісних діаграм утворюючих пристроїв.

Третій спосіб передбачає використання декількох антен, що перемикаються, тоді просторові напрямки по азимуту розбиваються на сектори. Зі збільшенням коефіцієнтів підсилення антен їх число зростає, а для розміщення великої кількості антен потрібно збільшувати габаритні розміри й масу всієї антенної системи. У цьому випадку можливий компромісний розв'язок, що забезпечує необхідне посилення й задовольняє ваго-габаритні обмеження.

Для його реалізації пропонується розмістити на борту дрона шість антен типу «хвильовий канал». З урахуванням ваго-габаритних обмежень конструкція однієї антени буде складатися лише із трьох елементів. Габаритні показники можна визначити використовуючи рис. 1.

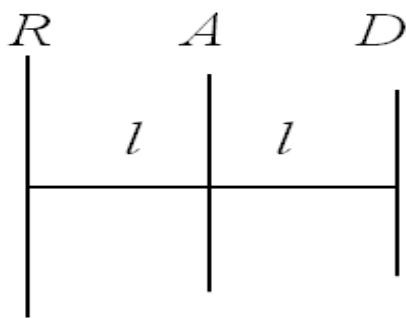


Рис. 1. Типова трьохелементна антена типу «хвильовий канал».

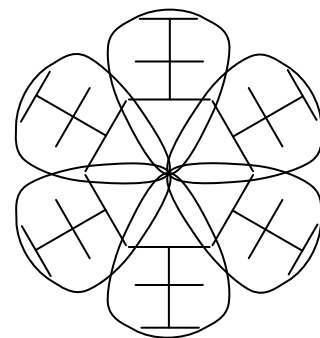


Рис. 2. Шести секторна антенна конструкція типу «хвильовий канал».

Відомо [4], що розміри елементів антени визначаються довжиною хвилі, а саме: активний вібратор $A = 0,5\lambda$; рефлектор незначно більше вібратора $R \geq A$; директор незначно менше його $D \leq A$; відстань між рефлектором, активним вібратором і директором $l = 0,25\lambda$. Для обраного частотного діапазону $\lambda = 0,125$ м, тому одна антена має габарити приблизно 7×7 см, конструкція із шести антен (рис. 2) вписується в окружність радіусом

$R_6 = 2l + l \sin 60 \approx 2,87l \approx 9$ см, а її вага складе близько 120 грам. Коефіцієнт підсилення трьохелементної антени типу «хвильовий канал» – 5,5 дБ. При наявності декількох антен на борту дрона виникає необхідність вибору антени, спрямованої у бік НКУ. Існує кілька варіантів реалізації подібної системи: перемикання виходу підсилювача передавача між антенами (один передавач, один підсилювач потужності, кілька антен); перемикання виходу передавача між підсилювачами потужності й антенами (один передавач, кілька сполучених підсилювачів потужності й антен); перемикання сигналу між передавачами (число передавачів і підсилювачів потужності дорівнює числу антен).

При першому варіанті вихідний сигнал підсилювача потужності комутується між декількома антенами. Гідністю цього варіанта є використання єдиного передавального модуля й підсилювача потужності для роботи на кілька антенних пристроїв. Загальним недоліком є втрати в комутуючому пристрої.

При другому варіанті число підсилювачів потужності дорівнює числу антен. До недоліків такого підходу можна віднести: наявність декількох підсилювачів потужності, які займають багато місця й мають більшу вагу.

Третій варіант вимагає використання для кожної антени свого передавача й підсилювача потужності. У цьому випадку перемикач сигналів виконується на рівні цифрової логіки. До переваг даного підходу слід віднести високу надійність системи. Однак платою за це є велика вага й висока вартість.

Очевидно, що для дронів кращим є перший варіант – тобто перемикання виходу підсилювача потужності передавача між антенами.

Таким чином, при використанні запропонованого варіанта побудови антенної системи для дронів загальне посилення приймально-передавального тракту може досягти 55 дБ, що забезпечить на віддаленні 10 км ВСШ на вході приймача 22 дБ, а відповідно – можливість високошвидкісної та якісної передачі інформації за рахунок використання, наприклад, модуляції QAM64 з імовірністю помилки порядку 10^{-8} . Високе значення ВСШ також може забезпечити стійке управління дронами, навіть при впливі навмисних завад, коли за рахунок використання простих алгоритмів модуляції: BPSK, QPSK, забезпечується пропускну здатність, достатня для передачі сигналів управління.

Література

1. Явіся В.С. Спосіб забезпечення високошвидкісної передачі даних безпілотними літальними апаратами // Одинадцята міжнародна науково-технічна конференція «Проблеми телекомунікацій». Матеріали конференції. – К.: КПІ ім. Ігоря Сікорського. – 2017. – С. 362-365.
2. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение, Изд. 2-е, испр.: Пер. с англ. / Б. Скляр. – М.: Издательский дом «Вильямс», 2003. – 1104 с.
3. Лысенко А.И., Явіся В.С. Способ обеспечения качества канала управления беспилотными летательными аппаратами // Научный журнал «Ученые записки ТНУ имени В.И. Вернадского. Серия: Технические науки». – Херсон: Гельветика. – 2017. – Т. 28 (67), № 1. – С. 23-26.
4. Гончаренко И.А. Антенны КВ и УКВ. Часть 3. Простые КВ антенны. М.: РадиоСофт, 2015. – 288 с.

АНАЛІЗ СПОСОБІВ ОТРИМАННЯ ДАНИХ ДЛЯ СИСТЕМ КЕРУВАННЯ ПОЛОЖЕННЯМ НАНОСУПУТНИКА

Явіся В.С., Явіся Д.В.

*Інститут телекомунікаційних систем КПП ім. Ігоря Сікорського, Україна
E-mail: yavisya@bigmir.net*

Analysis methods of data for nano satellite parameters of motion

Investigates methods of obtaining information about the parameters of movement of ultra-small spacecraft, which is necessary for the formation of the executive bodies of the control signals orientation and stabilization systems of spatial position. Traditional methods are evaluated in terms of their accuracy, feasibility, as well as the restrictions on weight and overall performance.

Відомо, що наносупутники (НС) можуть використовуватися як ретрансляційна мережа, для дистанційного зондування Землі, наукових місій, екологічного моніторингу, прогнозу землетрусів, дослідження іоносфери, у тому числі польотів до інших планет.

Незалежно від того, яка система стабілізації й орієнтації буде використовуватися, для її роботи необхідно одержати сигнали управління. Таке завдання вирішується як правило за допомогою інерційних систем [1].

Інерція є найбільш універсальним фактором, що дозволяє створити прилади для реєстрації зміни швидкості тіл у просторі. Такі прилади, називані акселерометрами або датчиками прискорень, дозволяють вимірювати проекцію на свою вісь чутливості прискорення тієї точки НС, де він встановлений. Акселерометр реагує тільки на сили, що прикладаються за посередництвом НС. Якщо одна зі складових загальної сили, що визначає прискорений рух НС, обумовлена дією тяжіння, то відповідна їй складова прискорення не може бути виміряна акселерометром. Сили тяжіння діють однаково як на прилад, так і на НС і тому при відсутності інших сил за допомогою акселерометра не можуть бути виявлені.

Таким чином, при русі НС у полі тяжіння вимірюване акселерометром прискорення відрізняється від дійсного й тому одержало назву *гаданого прискорення*. Вимір гаданого прискорення дозволяє визначити дійсне положення НС щодо центру тяжіння

Для управління необхідно знати три ортогональні складові вектора гаданого прискорення центру маси НС, тобто мати три датчики, встановлені у центрі маси НС, із трьома взаємно перпендикулярними осями чутливості. Ці осі чутливості повинні бути орієнтовані по тім осям координат, у яких заданий вектор положення центру маси НС щодо центру тяжіння R . Триєдр осей чутливості акселерометрів являє собою *осі вимірювальної системи*, а осі, у яких заданий вектор R – *інерційний координатний базис*, тобто базис, щодо якого відлічується абсолютне прискорення. Осі інерції (або осі форми) НС не збігаються з інерційним базисом, а обертаються щодо нього залежно від

напрямку вектора швидкості центру маси НС. Отже, для управління за допомогою виміру гаданих прискорень або *інерційного управління* необхідно або сполучати осі вимірювальної системи з інерційним координатним базисом незалежно від руху НС, або в кожний момент часу знати взаємне розташування осей вимірювальної системи й інерційного базису. В останньому випадку складові вектора гаданого прискорення з осей вимірювальної системи повинні бути перепроєктовані на осі інерційного координатного базису [2].

Таким чином, технічна реалізація методу інерційного управління можлива у двох варіантах. Перший – за допомогою пристроїв, які не обертаються разом із НС і, зберігаючи своє положення відносно інерційного базису, служать опорою для вимірювальної системи. Другий варіант – за допомогою пристроїв, які забезпечують обчислення параметрів, що визначають кути між осями вимірювальної системи й інерційного базису, а також проектування вимірюваних компонентів прискорення на осі цього базису.

Перший варіант вимагає наявності приладів, що фізично моделюють інерційний базис на борті НС, – гіростабілізованих платформ, другий – використання безплатформових систем.

При реалізації платформових систем забезпечення необхідної надійності й збільшення точності виявилось пов'язаним зі значним ростом маси й габаритів платформ, негативною є і їх чутливість до великих перевантажень і кутів обертання, що характерно для НС. Тому безплатформні інерційні системи (БІС), завдяки наявності сьогодні високошвидкісних обчислювальних пристроїв у мініатюрному виконанні, займають лідируюче положення при створенні нових систем управління об'єктами, для яких є критичними ваго-габаритні показники таких систем [2, 3].

При автоматизації системи стабілізації насамперед вирішується завдання демпфірування коливань НС, що виникають при зміні програми польоту й дії зовнішніх збурень.

Теорія повністю автоматизованої системи стабілізації, як і будь-якої системи автоматичного управління, містить математичний опис руху НС, який розглядається як об'єкт управління. Центральним завданням цієї теорії є обґрунтування вибору законів управління, тобто співвідношень, що зв'язують різницю між вимірюваними поточними й програмними значеннями параметрів руху НС із командами на органі управління. Закони управління в сучасних системах стабілізації НС, крім забезпечення точності, стійкості й певного характеру перехідного процесу в системі, повинні екстремізувати певні критерії [2].

У безплатформних системах стабілізації (БСС) зв'язок між інерційним і вимірювальним базисами виражається в процесі обчислень через параметри, які не можуть безпосередньо служити параметрами управління.

Специфіка БСС відносно математичного опису об'єкта стабілізації полягає в тому, що рівняння руху НС повинні бути записані через вимірювані датчиками параметри й через параметри зв'язку. Це спрощує замикання систем рівнянь стабілізації. І ще одна особливість БСС – необхідність розробки методів синтезу алгоритмів, що забезпечують обчислення параметрів зв'язку в

реальному часі, а також аналізу системи помилок, що супроводжують ці обчислення.

У цілому розробку БСС доцільно будувати таким чином, щоб незважаючи на її специфіку математичний опис окремих частин системи дозволив би при виборі закону управління використовувати ефективні й добре розроблені загальні методи теорії автоматичного управління й, зокрема, методи, які застосовуються в платформних системах. Саме для цього необхідно визначити метод, що дозволяє одержати сигнали управління, які забезпечують роботу виконавчих органів систем орієнтації й стабілізації положенням НС [2].

Первинна інформація про параметри кутового руху НС відповідно до законів механіки може бути отримана у вигляді прискорення крапки установки вимірювального приладу або інтегралів цього прискорення. Необхідно відзначити, що на будь-якому об'єкті, що рухається, можна безпосередньо (без зв'язку з іншими тілами) виміряти лише прискорення. Усі інші величини, що знімаються з датчиків, являють собою інтеграли від прискорення. З позицій загального komponування функціональної схеми БСС, а також для зручності формування вимог по точності доцільно розбити її на три підкласи залежно від співвідношення величин, які безпосередньо вимірюються й обчислюються [2]:

- системи, де вимірюються тільки лінійні прискорення, а всі інші параметри обчислюються;

- системи, де вимірюються, крім лінійних параметрів, і кутові швидкості;

- системи, де вимірюються будь-які параметри, включаючи й кути Ейлера.

Система на основі датчиків лінійних прискорень.

Для того щоб обчислити параметри кутового положення НС, необхідно знати його кутову швидкість відносно інерційного базису.

Для вимірювання кутової швидкості використовуються акселерометри з інтегральним виходом. Максимальна точність таких приладів характеризується помилкою близько 0,001% масштабного коефіцієнта [4]. Отже, помилка на одному такті обчислень кутової швидкості буде порядку 10^{-4} c^{-1} для плеча довжиною 1 м. При величині кроку дискретності 0,1 с помилка обчислень уже за 2-3 хвилини накопичується до величин, порівнянних з вимірюваними значеннями, що приводить до необхідності мати датчик з нестабільністю масштабного коефіцієнта не більш $10^{-6}\%$, на що розраховувати навіть у перспективі важко. Таким чином, система на основі одних датчиків лінійних прискорень поки представляє лише теоретичний інтерес.

Система з виміром лінійних прискорень і кутової швидкості.

Усі існуючі й перспективні високоточні датчики лінійних прискорень і кутових швидкостей дозволяють одержувати інформацію тільки у вигляді приросту інтегралів від названих параметрів, тобто, по суті, є датчиками приросту лінійної швидкості й кутів обертання НС. Але такі параметри, як лінійне прискорення й кутова швидкість, мають набагато більш глибокий фізичний зміст, ніж приріст їх інтегралів. Тому в цьому випадку можна говорити про існування двох методів:

- будувати математичний апарат паралельно для безпосередньої й інтегральної форми знімання інформації з вимірювальної системи;

- при розв'язку теоретичних питань вважати, що інформація про параметри руху доступна в дійсній розмірності останніх, а практично інтегральний її характер ураховується при розробці конкретних алгоритмів побудови інерційного координатного базису (ІКБ).

Для обчислення параметрів руху НС необхідно знати вектор прискорення його центру маси й вектор кутової швидкості обертання біля центру маси. Таким чином, вимірювальна система повинна мати, мінімум три датчики лінійних прискорень і три датчики кутової швидкості.

Система на основі датчиків, що вимірюють кути Ейлера.

Відлік кутів Ейлера проводиться від інерційного базису, тому його фізичне моделювання є неминучим. Однак у цьому випадку на відміну від звичайних платформних систем моделюються тільки вимірювальні осі, а не платформа для розміщення датчиків лінійних прискорень. Таким чином, для одержання інерційних компонентів вектора швидкості необхідно вимірювання, які здійснюються відносно зв'язаної системи координат, перераховувати до ІКБ.

Перевагою подібної системи є економія обчислювальних ресурсів при аналітичній побудові інерційного базису. Значним недоліком є обмеження максимальних кутів повороту й припустимих перевантажень через наявність вільних гіроскопічних систем на борті НС. Система з виміром кутів Ейлера може розглядатися як граничний випадок між платформним і безплатформним варіантами: по наявності фізичних моделей ІКБ на борті цю систему можна віднести до категорії звичайних інерційних, а по характеру розташування датчиків прискорення – до категорії безплатформних систем.

Відзначений недолік системи з вільними гіроскопічними приладами на теперішньому етапі розвитку інерційних систем управління зводить до мінімуму переваги БІС. Дійсно, у порівнянні з гіростабілізованою платформою зберігається перевага в забезпеченні надійності, а також у можливості використовувати датчик прискорення більших ваг і габаритів. Недоліком є необхідність мати на борті потужний обчислювач, що збільшує до того ж сумарну помилку побудови ІКБ.

Тому при побудові системи стабілізації НС для одержання керуючої інформації доцільно використовувати системи з виміром лінійних прискорень і кутової швидкості.

Література

1. Лисенко О.І., Явіся В.С. Аналіз методів отримання сигналів управління для систем орієнтації та стабілізації наносупутника // Науковий журнал «Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки». – Херсон: Гельветика. – 2017. – Т. 28 (67), № 2. – С. 31-37.
2. Лебедев Р. К. Стабилизация летательного аппарата бесплатформенной инерциальной системой. – М.: Машиностроение, 1977. – 144 с.
3. Гуцин В.Н. Основы устройства космических аппаратов. – М.: Машиностроение, 2003 г. – 272 с.
4. Литвин М.А., Малюгина А.А., Миллер А.Б. Типы ошибок в инерциальных навигационных системах и методы их аппроксимации // Информационные процессы. – 2014. – Том 14. – № 4. – С. 326–339.

БАЛАНСИРОВКА ЭНЕРГЕТИЧЕСКИХ ХАРАКТЕРИСТИК СЕНСОРОВ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

Осинский А.К., Петрова В.Н.

Институт телекоммуникационных систем

КПИ им. Игоря Сикорского, Украина

E-mail: toni02133@gmail.com

Balancing the energy performance of sensors in wireless sensor networks

The paper proposed a method of balancing the energy characteristics of sensors in wireless networks. The method is based on the use of energy in the radio range of sensors transmitting data. The currently inactive sensors can receive and detect data packets and use them to recharge the power supply. Energy efficiency is determined by the accuracy of matching the receiving antenna with the input circuit and the voltage drop across the rectifier module. The analysis of relative losses depending on the frequency for a typical antenna of the wireless range.

Актуальность работы обусловлена все более широким распространением беспроводных сенсорных сетей и необходимостью продления срока их жизни, которая определяется в основном разрядом встроенного в сенсор источника питания. Целью работы является разработка метода балансировки энергетических характеристик сенсоров в беспроводной сети [1-2].

Типовое потребление энергии различными блоками сенсора представлено на рис.1. На чувствительный элемент тратится около 4 % от суммарного энергопотребления. В то же время 90 % энергии расходуется на организацию радиосвязи с соседними узлами или базовой станцией в зависимости от используемого протокола обмена.

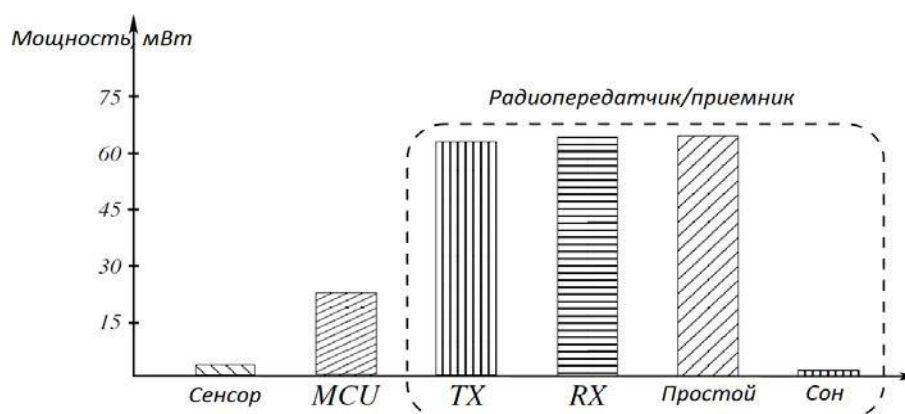


Рис. 1. Распределение потребления энергии сенсора [1].

С точки зрения энергоэффективности в БСС наибольший практический интерес представляют модификации базового протокола передачи данных – *Low Energy Adaptive Clustering Hierarchy (LEACH)*, который представляет

собой TDMA-протокол с адаптивной кластеризацией. Задача протокола – минимизация энергии, необходимой для создания и обслуживания динамически организуемых кластеров сенсоров. LEACH является иерархическим протоколом, в котором сенсоры передают данные вершине кластера, где происходит накопление и компрессия данных, и далее их передача базовой станции. LEACH-протокол предполагает, что каждый сенсор имеет запас энергии достаточный для передачи данных непосредственно базовой станции или ближайшей вершине кластера.

Балансировка энергопотребления в сенсорной сети осуществляется как за счет применения более сложных алгоритмов, учитывающих запас энергии каждого узла, так и за счет подзарядки источников питания наиболее разряженных узлов непосредственно от беспроводного интерфейса.

В неактивном состоянии приемная часть каждого узла, не участвующего в кластере, может принимать и накапливать энергию пакетов беспроводного интерфейса. При использовании диапазона 2,4 ГГц и достаточно большом числе узлов, участвующих в обмене данными с базовой станцией и соседними узлами, энергии, принимаемой неактивными сенсорами, достаточно для эффективной подзарядки сенсора. Накопление энергии может происходить на конденсаторе достаточно большой емкости (ионисторе), после разряда, которого при переходе сенсора в активный режим происходит его переключение на основной неперезаряжаемый источник питания.

Основные потери энергии в данном случае обусловлены большим расстоянием между источником и приемником сигнала сети (обычно более 10 м), низким трафиком в сети и несогласованностью импеданса приемной антенны с входным контуром.

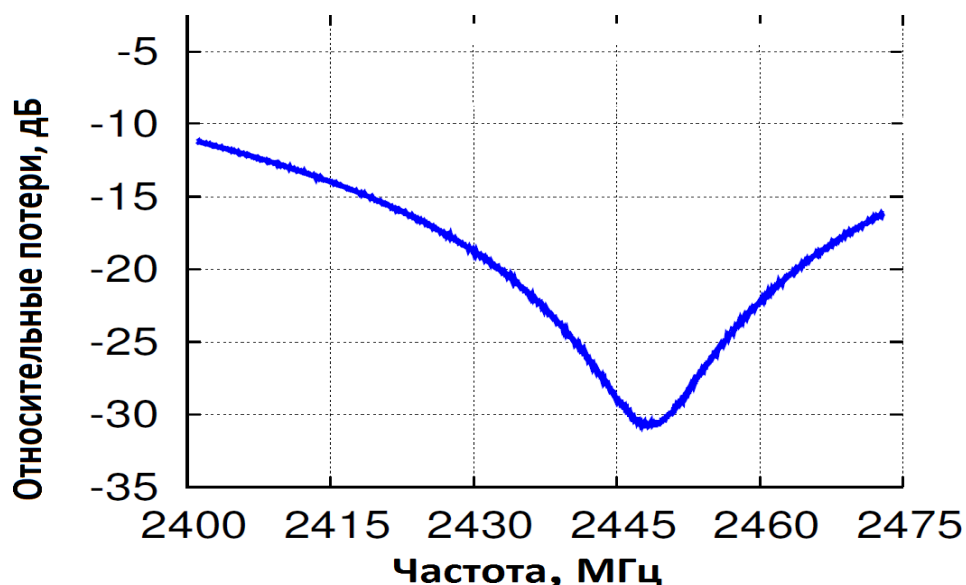


Рис. 2. Относительные потери во входном контуре.

На рис. 3 приведена зависимость потерь от частоты для типовой антенны сенсора, работающей в диапазоне Wi-Fi 2,4 ГГц. Как можно

заметить, во всем диапазоне относительные потери не превышают 10дБ. Минимум потерь наблюдается в диапазоне 2,401–2,473 ГГц (Рис.2).

Мощность на выходе выпрямителя определяется потерями в выпрямителе и расстоянием от базовой станции. Потери в данном случае обусловлены наличием порогового падения напряжения на СВЧ-диодах. На рис. 3 показана выходная мощность на выпрямителе как функция от мощности радиосигнала при удалении от базовой станции. Результаты представлены для трех различных каналов Wi-Fi диапазона.

При максимальной мощности радиосигнала на выходе выпрямителя мощность достигает 100 мкВт для всех трех каналов. При увеличении расстояния до базовой станции и уменьшении мощности радиосигнала мощность на выходе выпрямителя падает экспоненциально до уровня менее 1 мкВт при мощности радиосигнала – 17 дБм.

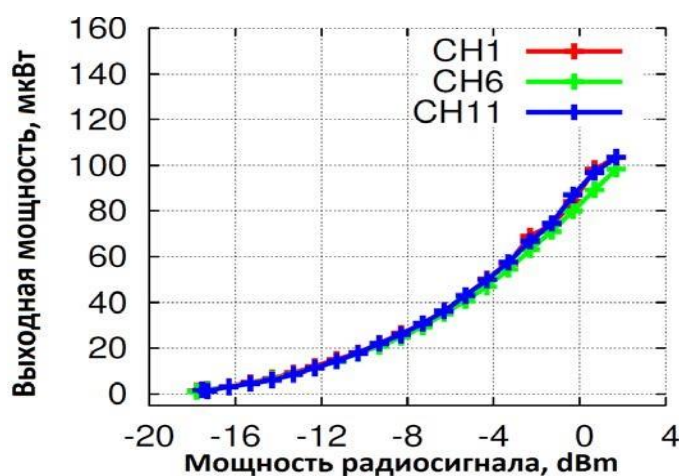


Рис. 3. Зависимость мощности на выходе выпрямителя в зависимости от мощности радиосигнала.

Выводы. Использование при организации подсистемы питания сенсоров БСС энергии беспроводного интерфейса позволяет существенно увеличить время жизни сети и повысить ее надежность за счет перераспределения энергии между сенсорами. Такой подход особо эффективен для БСС, регистрирующих событие, когда 99 % времени сенсоры находятся в режиме ожидания. За время ожидания накопительный элемент сенсора может быть полностью заряжен при наличии интенсивного информационного обмена между близлежащими элементами БСС.

Литература

1. Akyildiz, F. Wireless sensor networks: a survey / F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci // Computer Networks. – 2002. – № 38(4). – P. 393–422.
2. Reshma, I. Leach Protocol in Wireless Sensor Network: A Survey. Tandel, Shri S'adVidya / I. Reshma. – Guja- rat, India : Mandal Institute of Technology, 2016. – P. 1894–1896.

ВИЗНАЧЕННЯ ВЗАЄМНОГО РОЗТАШУВАННЯ УГРУПОВАННЯ КВАДРОКОПТЕРІВ ПІД ЧАС МОНІТОРИНГУ НАЗЕМНОЇ ОБСТАНОВКИ В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

Якорнов Є.А., Цуканов О.Ф.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: cukanov-o@ukr.net

Determination of mutual location of the grouping of quadrocopters during monitoring of the territorial situation in emergency situations

Methods for determining the coordinates of a group of quadrocopters in a ground-based control system for monitoring the situation in emergency response areas are presented.

В даний час, безпілотні літальні апарати (БПЛА) знаходять все більш широке застосування в бездротових сенсорних мережах і, зокрема, при автоматизованому зборі даних і подальшою передачею їх через Інтернет з віддалених сенсорних вузлів, які накопичують інформацію за час автономної роботи, що дозволяє завчасно запобігти будь-яким стихійним лихам або використовувати інформацію з сенсорів в сільськогосподарській галузі [1] (рис. 1).

Однак, в разі непередбачених надзвичайних ситуацій (НС) для їх моніторингу необхідної інформацією та прийняття рішення на ліквідацію наслідків НС є дані про поточний стан в реальному масштабі часу. Причому, чим детальніше буде ця інформація, тим краще можна буде оцінити обстановку, визначити задум, скласти план ліквідації НС, визначити завдання та організувати взаємодію між підрозділами, які беруть участь в ліквідації НС.

Використання в якості БПЛА квадрокоптера (КК) істотно розширює функціональні можливості мереж, особливо при моніторингу наземної обстановки в зоні НС.

При цьому, на перший план висувається завдання фіксації місця розташування КК. Тому для забезпечення роботи мережі в складі кількох КК (рис.1) необхідно знати з високою точністю координати кожного КК на місцевості і між собою [2].

Координати КК можуть бути визначені кількома способами:

- 1) з використанням трьох рознесених наземних пунктів вимірювання координат (НПВК) і наземної системи управління (СУ) КК;
- 2) з використанням чотирьох рознесених НПВК і наземної СУ КК;
- 3) за допомогою одного наземного НПВК і датчиками GPS які встановлені на борту кожного КК;

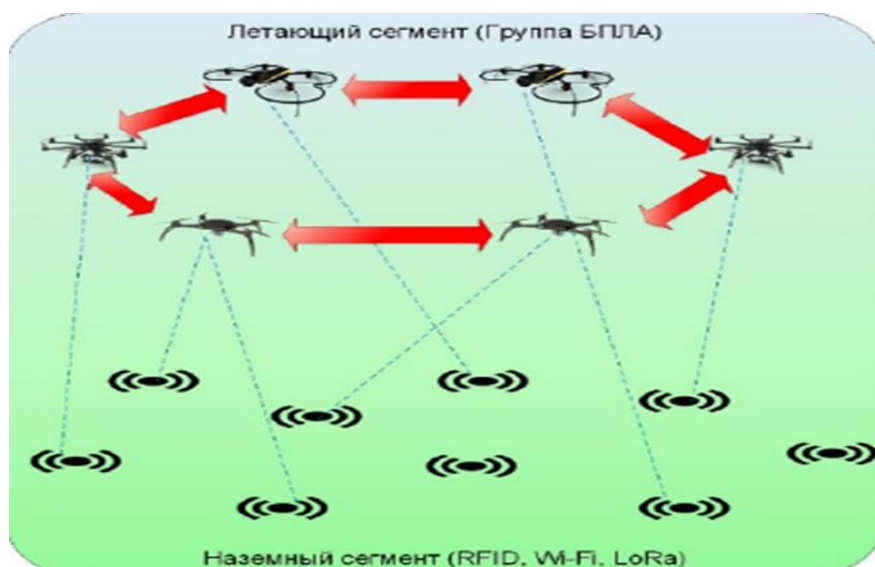


Рис.1.

4) за допомогою одного наземного НПВК і датчиків GPS встановлених на борту кількох КК які є базовими, а на інших - датчиків вимірювання взаємних відстаней [2].

Перший спосіб визначення параметрів розташування КК складається з трьох НПВК і СУ. Кожен КК за запитом з СУ випромінює сигнал, який приймається трьома НПВК. Час приходу сигналів на СУ це інформація про відстань до конкретного КК. Сигнали з КК мають інформаційну частину за допомогою якої здійснюється ідентифікація конкретного КК. Координати установки позиціонування визначаються за методом трьох діяльностей.

У другому способі, реалізується різностно-далекомірний метод за допомогою чотирьох НПВК (один з них опорний). В цьому випадку СУ випромінює сигнал запиту на вимірювання параметрів розташування, після чого сигнали від кожного КК приймаються чотирма наземними прийомними пунктами. При цьому визначаються різниці дальностей, а саме: різниці між дальностями до кожного КК і дальностями до опорного НПВК.

У третьому способі координати визначаються за допомогою датчиків GPS, встановлених на борту кожного КК, і за запитом з СУ передається на неї.

Четвертий спосіб, дозволяє зменшити кількість датчиків GPS за рахунок визначення координат на борту КК шляхом вимірювання взаємних відстаней між ними і робить угруповання КК автономнішою. При цьому інформація про координати КК передається на один з базових КК, а далі на СУ. За допомогою датчиків системи GPS здійснюється прив'язка до обраної системи координат, а координати інших КК вимірюються шляхом вимірювання взаємних відстаней за рівнем потужності прийнятого сигналу від сусідніх КК [3].

Перевагою першого способу є простота і висока автономність роботи. Прив'язка до місцевості здійснюється шляхом прив'язки безпосередньо НПВК. При цьому бортова апаратура КК істотно спрощується і споживає мінімум електроенергії, що збільшує час польоту КК. До недоліків відноситься складність наземної апаратури, яка передбачає наявність трьох НПВК і окремо СУ.

Перевагами третього і четвертого способів є поєднання функцій СУ з НПВК, які приймають інформацію про координати від кожного КК і на основі отриманої інформації здійснюється їх супровід. При цьому істотно зменшується час розгортання угруповання КК в районі ліквідації НС.

Таким чином, переваги третього і четвертого способів очевидні. Однак вони не завжди працездатні через умови наземної обстановки в зоні НС. Саме тому на практиці для ефективного управління угрупованням КК необхідно мати можливість застосування комбінації всіх чотирьох способів визначення координат.

Література

1. Шкляева А.В., Киричек Р.В., Кучерявый А.Е. Методы тестирования летающих сенсорных сетей // Информационные технологии и телекоммуникации. 2016. Том 4 № 2. с. 43-52.
2. Якорнов Є.А., Цуканов О.Ф. Визначення параметрів руху маневруючих безпілотних літальних апаратів у мережах FANET. // Матеріали XIII-ої Міжнародної науково-технічної конференції «Перспективи телекомунікацій» (ПТ-19) К.: НТУУ «КПІ ім. І.Сікорського», 2019, с. 285 – 287.
3. Якорнов Є.А., Цуканов О.Ф. Визначення координат сенсорів бездротової сенсорної мережі. // Матеріали XII-ої Міжнародної науково-технічної конференції «Перспективи телекомунікацій» (ПТ-18) К.: НТУУ «КПІ ім. І.Сікорського», 2018, с. 361 – 363.

РАЗВИТИЕ АЛГОРИТМОВ МАРШРУТИЗАЦИИ В МОБИЛЬНЫХ СЕНСОРНЫХ СЕТЯХ

Штойко А.А., Петрова В.Н.

*Институт телекоммуникационных систем, Национальный Технический
Университет Украины имени Игоря Сикорского, Киев, Украина
E-mail: shtoyko1999@gmail.com*

Development of Routing Algorithms in Mobile Touch Networks

Mobile networks are one of the most promising areas for the development of information and communication networks. This article discusses existing and emerging routing protocols in wireless networks.

Беспроводная сенсорная сеть – это самоорганизующаяся сеть датчиков (сенсоров) объединённых между собой посредством радиоканала. Каждый элемент представляет собой устройство, состоящее из накопителя данных, вычислительно модуля и источника питания. В зависимости от решаемой задачи сенсоры могут представлять собой различные датчики, например: температуры, давления, освещённости [1].

Как известно из стандартных протоколов существует ряд проблем, которые в разных ситуациях становятся препятствием для решения задач поставленные сенсорной сети. В последнее время было проведено ряд исследований [2-5] для устранения недостатков, а именно:

- 1) Алгоритмы «рандеву» для беспроводных сенсорных сетей.
- 2) Алгоритм автоматической конфигурации адресного пространства для беспроводной сенсорной сети на основе разделения координаторов.
- 3) Алгоритм динамического выделения адресов для управления и контроля в беспроводных сенсорных сетях.

В работе [2] рассматривается задача оптимизации сбора информации с узлов сенсорной сети, который осуществляется мобильной базовой станцией (МБС). Подобный подход к сбору информации обещает заметно экономить на энергопотреблении при передаче данных.

Было доказано, что наиболее эффективным путем движения МБС для сбора информации есть периметр зоны работы сети, но данный маршрут есть неэффективным для узлов сети. Кроме того тратится энергия на поддержание информации (о топологии и адресном пространстве сети) в актуальном состоянии.

Однако главной загвоздкой является задержка, которая возникает при получении информации из-за невысокой скорости передвижения мобильной станции, поэтому предлагается следующий подход. Особый класс устройств,

называемый точками «рандеву», должен принимать данные от источников отправителей, накапливать их и передавать их мобильной станции в момент её нахождения в действии точки «рандеву». Данный подход совмещает преимущества сбора информации с помощью использования МБС и кеширования данных внутри сети.

Общая схема работы алгоритма «рандеву» изображена на рис.1. Для примера возьмём поле размером 500 м^2 , на котором расположены узлы беспроводной сенсорной сети. Сбор информации производится МБС со средней скоростью $0,5 \text{ м/с}$. При такой скорости для посещения 100 произвольных узлов на поле понадобится около двух часов, но если использовать точки «рандеву», которые находятся в радиусе 100 м от центра поля, то для сбора информации потребуется около 20 минут.

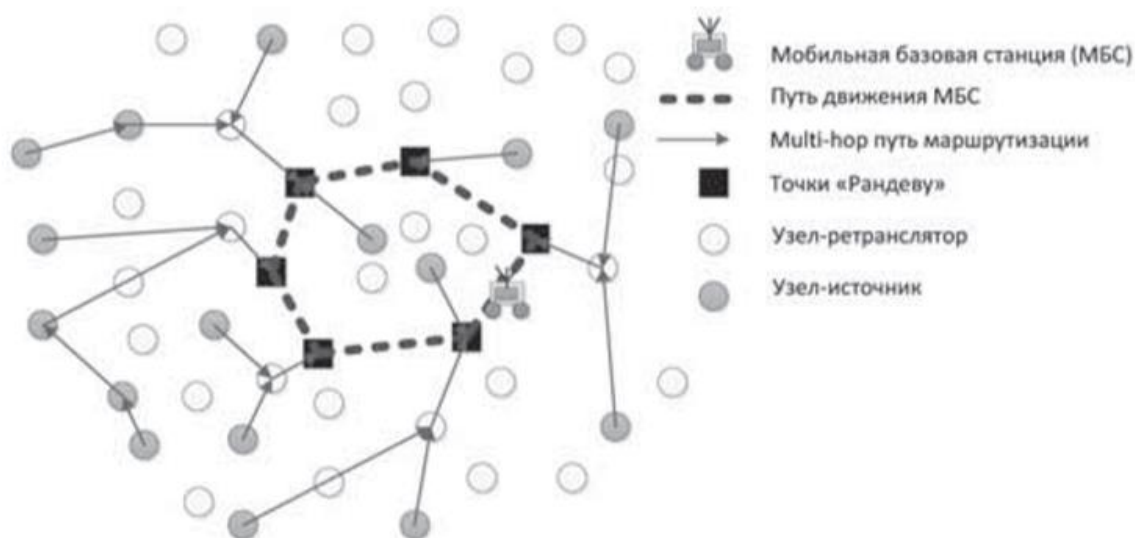


Рис.1. Общая схема работы алгоритма «рандеву».

Одной из существующих проблем является длительность жизни беспроводных сенсорных сетей, соответственно целью – увеличение жизни сети за счёт алгоритмов маршрутизации. Для достижения поставленной цели определена следующая задача: необходимо разработать модель для исследования алгоритмов многопутевой маршрутизации с учетом устранения дисбаланса энергопотребления в транзитных узлах БСС.

Рассмотрим сеть, состоящую из m узлов маршрутизации. В рамках базовой модели конфигурация сети описывается с помощью графа $G_s = (V_s, E_s)$, где $V_s = \{ \alpha_1, \alpha_2, \alpha_3, \dots, \alpha_m \}$ - множество узлов маршрутизации сети, $E_s = \{ \beta_1, \beta_2, \beta_3, \dots, \beta_n \}$ - множество каналов связи (рис. 2). Для каждого канала связи $(i,j) \in E_s$ задана его пропускная способность $c_{i,j}$. Величина $x_{i,j}$ характеризует долю входного трафика, протекающего в канале $(i,j) \in E_s$.

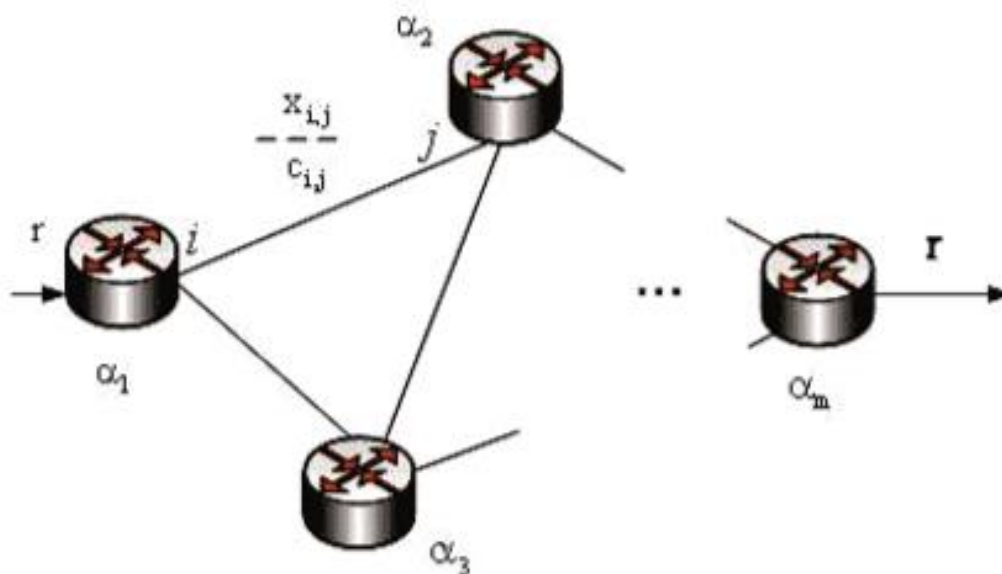


Рис. 2. Пример графа для описания сети.

Таким образом, на сегодняшний день существует множество проблем в области создания беспроводных самоорганизующихся сетей с переменной топологией. Одной из главных является проблема маршрутизации. Каждый тип протоколов маршрутизации потенциально имеет свои преимущества и недостатки при различных условиях.

Литература

1. Сергиевский М. WSN // Компьютер пресс. – 2007.
<http://www.compress.ru/article.aspx?id=17950&iid=831>.
2. Guoliang X., Tian W., Weijia J., Minming L. Rendezvous Design Algorithms for Wireless Sensor Networks with a Mobile Base Station // MobiHoc, Hong Kong. – 2011.
3. Shin H., Talipov E., Cha H. IPv6 Lightweight Stateless Address Autoconfiguration for 6LoWPAN Using Color Coordinators // 2009 IEEE International Conference on Pervasive Computing and Communications – March, 2009.
4. Yao Z., Dressler F. Dynamic Address Allocation for Management and Control in Wireless Sensor Networks. // 40th Annual Hawaii International Conference on System Science (HICSS'07). – January, 2007.
5. PalChaudhuri S., Du S., Saha A.K., Johnson D.B. A Stateless Addressing and Routing Architecture for Sensor Networks // 18th International Parallel and Distributed Processing Symposium (IPDPS'04) – Workshop 12, - April, 2004.

ОГЛЯД КОНЦЕПЦІЇ ПОТОКОВОЇ ОБРОБКИ ДАНИХ

Ковбаса А.О., Лисенко О.І.

Інститут телекомунікаційних систем КПП ім. Ігоря Сікорського, Україна

E-mail: antonkovbasa@gmail.com, lysenko.a.i.1952@gmail.com

Overview of the Streaming Data Processing concept

The idea of structuring data as a stream of events is nothing new, and it is used in many different fields. Even though the underlying principles are often similar, the terminology is frequently inconsistent across different fields, which can be quite confusing. This article tries to give understanding of the topic and make comparison with other concepts of data processing.

Існує велика плутанина щодо того, що означає потокова обробка даних. Багато визначень поєднують деталі імплементації, вимоги до продуктивності, моделі даних та багато інших аспектів інженерії програмного забезпечення. Світ потокової обробки все ще розвивається, і те, що конкретна популярна реалізація робить специфічні деталі або має певні обмеження, не означає, що ці деталі є невід'ємною частиною обробки потоків даних.

Почнемо спочатку: що таке потік даних (також його називають потоком подій)? Перш за все, потік даних - це абстракція, що представляє необмежений набір даних. Необмежений означає нескінченний і постійно зростаючий. Набір даних необмежений, оскільки з часом нові записи постійно надходять. Це визначення використовується Google, Amazon та майже всіма іншими компаніями. Зауважимо, що ця проста модель (потік подій) може бути використана для представлення майже будь-якої діяльності, яку ми хочемо проаналізувати. Ми можемо переглянути потік транзакцій між кредитними картками, фондові торги, доставку пакетів, мережеві події, що проходять через комутатор, події, про які повідомляють датчики на виробничому обладнанні, електронні листи, що надсилаються, переміщення в грі, тощо. Перелік прикладів нескінченний, тому що досить багато процесів можна розглядати як послідовність подій.

Окрім необмеженості, існує кілька інших атрибутів моделі поточкових подій:

***Потоки подій упорядковані.** Існує невід'ємне поняття, які події відбуваються до або після інших подій. Це стає більш зрозумілим якщо дивитися на фінансові події. Послідовність, коли я спочатку кладу гроші на свій рахунок і пізніше витрачаю гроші, сильно відрізняється від послідовності, в якій я спочатку витрачаю гроші, а пізніше покриваю борг, повертаючи гроші банку. Останній буде стягувати плату за овердрафт, а перший - ні. Зауважимо, що це одна з відмінностей між потоком подій та таблицею баз даних: записи в

таблиці завжди вважаються не упорядкованими, а інструкція «*order by*» в SQL не є частиною реляційної моделі.

***Незмінні записи даних.** Події, що відбулися, ніколи не можуть бути змінені. Фінансова операція, яка скасовується, не видаляється. Натомість у потік записується додаткова подія, яка записує скасування попередньої транзакції. Коли клієнт повертає товар у магазин, ми не видаляємо той факт, що товар був проданий йому раніше, а ми фіксуємо повернення як додаткову подію. Це ще одна різниця між потоком даних та таблицею баз даних - ми можемо видалити або оновити записи в таблиці, але це все додаткові транзакції, що відбуваються в базі даних, і як такі можуть бути записані в потоці подій, що реєструє всі транзакції.

***Потоки подій можна відтворити.** Це бажана властивість. Хоча легко уявити потоки, які не відтворюються (пакети TCP, що передаються через сокет, як правило, не підлягають повторенню), для більшості бізнес-програм важливо мати можливість відтворювати необроблений потік подій, що відбувалися місяцями (а іноді й роками) раніше. Це необхідно для того, щоб виправити помилки, спробувати нові методи аналізу, або проведення перевірок.

Варто зазначити, що ні визначення потоку подій, яке ми дали спочатку, ні атрибути, які ми згодом перераховували, нічого не говорять про дані, що містяться в подіях, або про кількість подій в секунду. Дані відрізняються для кожного окремого випадку - події можуть бути крихітними (часом лише кілька байтів) або дуже великими (повідомлення XML з багатьма заголовками); вони також можуть бути повністю неструктурованими, парами ключ-значення, напівструктурованими JSON або структурованими повідомленнями Avro або Protobuf. Хоча часто вважається, що потоки даних є "великими даними" і включають мільйони подій в секунду, ті ж методи, застосовуються однаково добре (і часто краще) для менших потоків подій, що мають лише кілька подій в секунду або хвилину.

Тепер, коли ми знаємо, що таке потоки подій, саме час переконатися, що ми розуміємо потокову обробку. Потокова обробка подій - це парадигма програмування - подібно до запиту-відповіді та пакетної обробки. Давайте розглянемо, як порівнюються різні парадигми програмування, щоб краще зрозуміти, як обробка потоків вписується в архітектуру програмного забезпечення:

***Запит-відповідь.** Це парадигма з найменшою затримкою, з часом відгуку в діапазоні від субмілісекунд до декількох мілісекунд, зазвичай з очікуванням того, що час відгуку буде в високим ступенем узгодження. Режим обробки зазвичай блокується - додаток відправляє запит і чекає відповіді від системи обробки. У світі баз даних ця

парадигма називається обробкою онлайн-транзакцій (OLTP). Системи продажів, обробки кредитних карт і системи відстеження часу зазвичай працюють в цій парадигмі.

***Пакетна обробка.** Це варіант високої затримки/високої пропускної здатності. Система обробки прокидається у встановлений час - щодня о 2:00, щогодини і т. д. Вона зчитує всі необхідні дані (або всі дані, доступні з моменту останнього виконання, всі дані з початку місяця тощо), записує весь необхідний вихід і чекає до наступного разу, коли її буде запущено. Часи обробки варіюються від хвилин до години, і користувачі розраховують прочитати застарілі дані під час перегляду результатів. У світі баз даних - це сховища даних та системи бізнес-аналізу - дані завантажуються величезними партіями раз на день, створюються звіти, і користувачі переглядають ті самі звіти до наступного завантаження даних. Ця парадигма часто має велику ефективність, але останніми роками підприємства потребують наявних даних у більш короткі терміни, щоб зробити прийняття рішень більш своєчасним та ефективним.

***Потокова обробка.** Це неблокуючий варіант. Заповнення розриву між світом запитів-відповідей, в якому ми чекаємо подій, для обробки яких потрібно дві мілісекунди, і світом пакетної обробки, в якому дані обробляються один раз в день і для їх завершення потрібно вісім годин. Більшість бізнес-процесів не вимагають негайної відповіді протягом мілісекунд, але також не можуть чекати наступного дня. Більшість бізнес-процесів відбуваються безперервно, і до тих пір, поки бізнес-звіти постійно оновлюються, а лінійка бізнес-додатків може безперервно відповідати, обробка може тривати, і ніхто не буде чекати конкретної відповіді протягом мілісекунд. Бізнес-процеси, такі як оповіщення про підозрілі кредитних операціях або мережеву активність, коригування цін в режимі реального часу на основі попиту і пропозиції або відстеження поставок пакетів - все це природно підходить для безперервної, але неблокуючої обробки.

Література

1. Martin Kleppmann, "Making Sense of Stream Processing" Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol.
2. Neha Narkhede, Gwen Shapira, and Todd Palino, "Kafka: The Definitive Guide" Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol.
3. Клеппман М. Высоконагруженные приложения. Программирование, масштабирование, поддержка. — СПб.: Питер, 2018. — 640 с.: ил. — (Серия «Бестселлеры O'Reilly»).

РОЗВИТОК ЕНЕРГОЗБЕРІГАЮЧОГО МЕТОДУ МОНІТОРИНГУ ЦІЛЕЙ У ЗОНАХ СПОСТЕРЕЖЕННЯ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ

Новіков В.І., Спаравало М.К., Лисенко О.І., Алексєєва І.В.

Інститут телекомунікаційних систем КІП ім. Ігоря Сікорського, Україна

E-mail: novikov1967@ukr.net, lysenko.a.i.1952@gmail.com

Development of the energy-saving method for monitoring purposes in the control areas of wireless sensor networks

Development of the energy-saving method for wireless sensor networks, in which the construction of the network topology is carried out by controlling the transmit power of the nodes WSN.

Перспективність і актуальність використання технології безпроводових сенсорних мереж (БСМ) для вирішення широкого кола завдань моніторингу та управління в різних областях, таких як автоматизація підприємств, безпека, екологія, надзвичайні ситуації залучили до досліджень провідні наукові центри та лабораторії світу. Однак існують проблеми, які перешкоджають масовому впровадженню рішень на базі БСМ. Одна з них – це необхідність збільшення часу автономної роботи безпроводової мережі. Так як живлення вузлів БСМ здійснюється від батарей обмеженої ємності, то задача управління витратами енергоресурсу сенсорних вузлів є однією з основних. Для цього до складу системи управління БСМ [1] входить підсистема управління витратами енергоресурсу. Метою її функціонування є мінімізація та перерозподіл витрат енергоресурсу вузлами для максимізації тривалості функціонування БСМ.

Управління витратами енергоресурсу вузлів БСМ може бути реалізоване за рівнями еталонної моделі OSI з використанням різних методів, які в загальному випадку можна поділити на дві групи: методи збереження енергії батарей і методи управління потужністю передачі. В роботі [2] запропоновано новий енергозберігаючий метод моніторингу цілей у зонах спостереження сенсорів БСМ, який відноситься до першої групи методів.

Для підвищення ефективності енергозберігаючого методу моніторингу цілей в роботі [3] запропоновано використати в ньому нову енергозберігаючу процедуру побудови топології мережі шляхом управління потужністю передачі вузлів БСМ. Оцінка ефективності запропонованого енергозберігаючого методу моніторингу цілей у зонах спостереження БСМ включає наступні етапи:

1. Аналіз умов функціонування мережі і завдання початкових даних у вигляді: параметри БСМ (розмірність мережі: N – кількість вузлів мережі, Z – кількість цілей, діаметр мережі і площа розміщення); параметри вузлів

(початкові координати розміщення на місцевості – x_i, y_i , CV – середній ступінь зв'язності мережі, E^{δ} – початковий енергетичний резерв сенсорів, $e^{Пд}, e^{Пр}, e^M$ – енергія, що необхідна для передачі, прийому та моніторингу однієї одиниці даних, F – швидкість (частота) передачі даних, t_{ij} – загальний час спостереження i -го сенсора за j -ою ціллю).

2. Вибір показників ефективності функціонування БСМ. З позицій системного підходу необхідно оцінювати ефективність енергозберігаючої методики моніторингу за двома групами показників.

Глобальний показник. Моніторинг виступає в ролі підсистеми системи управління БСМ і тому, очевидно, необхідно оцінювати його ефективність за показниками функціонування самої мережі: тривалість функціонування мережі – $T_{\Phi_{БСМ}} = \max \{ \min T_{\Phi_i} \}$ – тривалість роботи мережі до моменту відмови вузла через нульову ємність його батареї. В загальному випадку $T_{\Phi_{БСМ}}$ повинно визначатися відсотком працюючих сенсорів, які дозволяють виконувати функції БСМ. Але для порівняння з іншими методами тривалість функціонування мережі буде визначати надане визначення.

Локальні показники (L_1, L_2, L_3). Метод моніторингу вимагає додаткових тимчасових витрат і ресурсів мережі для передачі службової інформації, а також ресурсів зберігання і обчислення сесій спостереження. Тому необхідно оцінити ефективність за наступним локальними показниками:

- L_1 – алгоритмічна складність;
- L_2 – зв'язна складність (кількість повідомлень необхідних для реалізації процедури збору та розсилки інформації);
- L_3 – складність зберігання (об'єм необхідної пам'яті).

3. Проведення досліджень. Оцінка ефективності методики моніторингу проводиться з використанням наступних вихідних даних: розмірність мережі: $N = 100$, $M = 5 - 20$, енергія необхідна для передачі однієї одиниці інформації – 0, 12 мВт (100 м) – 36,3 мВт (400 м); енергія необхідна для прийому однієї одиниці інформації – 0,1 мВт. Протокол доступу до каналу – детермінований.

Оцінка ефективності методу моніторингу цілей за локальними та глобальними показниками проводилася в порівнянні з існуючим методом surveillance method (SM) та без використання методів моніторингу [5].

Результати дослідження оцінки ефективності розробленого методу моніторингу у порівнянні з існуючим методом SM та без використання методів моніторингу представлені на рис. 1.

На рис 1. зображено залежність тривалості функціонування БСМ $T_{\Phi_{БСМ}}$ від радіусу моніторингу R_M при різних кількості цілей та при використанні різних методів. Зі збільшенням R_M тривалість функціонування збільшується за рахунок збільшення кількості сенсорних вузлів потенційно здатних спостерігати за цілями, що доводить перевагу запропонованого методу моніторингу.

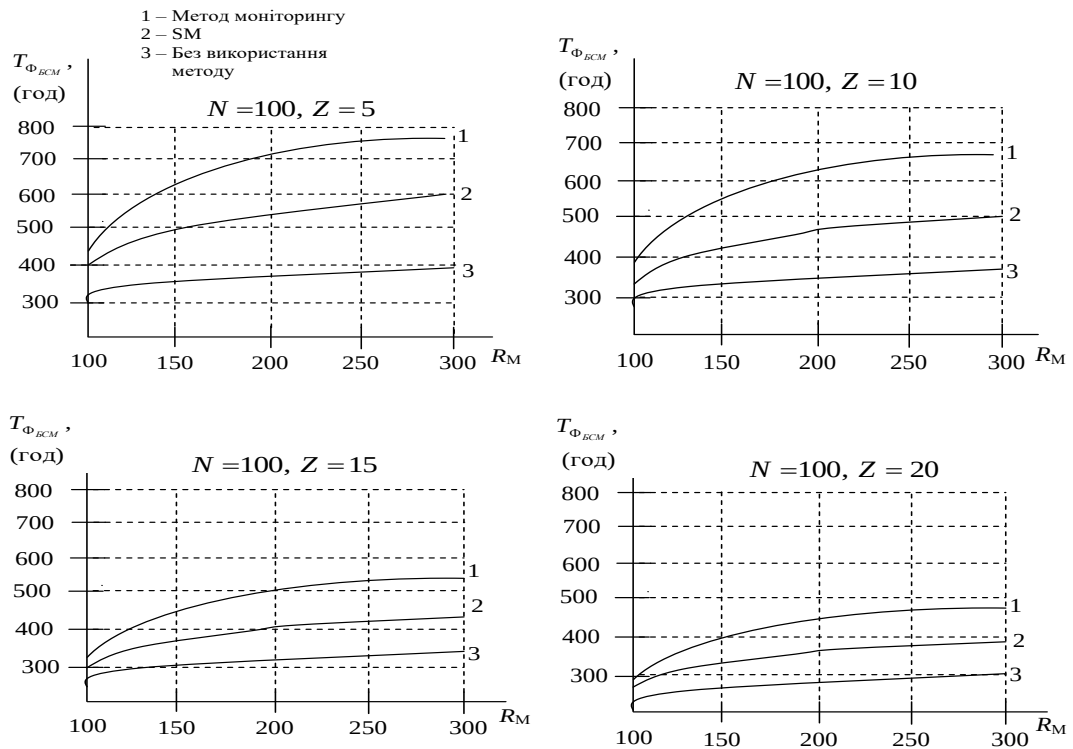


Рис. 1. Залежність тривалості функціонування $T_{\Phi_{БСМ}}$ сенсорної мережі від радіусу моніторингу, кількості цілей та методів моніторингу ($R_{\Pi} = const$).

Отримані результати показують, що застосування запропонованого методу забезпечує збільшення тривалості функціонування БСМ в середньому на 10-15% в порівнянні з існуючими методами.

Література

1. Лисенко О. І. Функціональна модель системи управління безпроводовою сенсорною мережею із самоорганізацією для моніторингу параметрів навколишнього середовища / О. І. Лисенко, К. С. Козелкова, В. І. Новіков, Т. О. Прищепа, А. В. Романюк // Системи обробки інформації. - 2015. - Вип. 10. - С. 222-225
2. Новіков В. І. Метод збільшення часу життя безпроводної сенсорної мережі з надлишковою кількістю вузлів під час стеження за цілями моніторингу / В. І. Новіков // Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. - 2017. - Том 28 (67) № 2 - С. 38-43.
3. Алексеева І.В. Математична модель процедури побудови енергозберігаючої топології безпроводної сенсорної мережі моніторингу цілей / І.В. Алексеева, О.І. Лисенко, В.І. Новіков / Міжнародна науково-технічна конференція „Проблеми телекомунікацій”. – К.: КПІ ім. Ігоря Сікорського, 2018. – С. 316 – 319.
4. Yan T. Differentiated surveillance for sensor networks / T. Yan, T. He, J. A. Stankovic // 1st Int. Conf. Embedded Networked Sensor Systems. – Los Angeles. –2003. – pp. 51 – 62.
5. Жук О.В. Оцінка ефективності методики моніторингу цілей в безпроводній сенсорній мережі тактичної ланки управління / О.В. Жук, В.А. Романюк, О. Я. Сова // Труды Академії. – 2008. – № 7 (87). – С. 154 – 162.

РОЗВИТОК МЕТОДІВ ЕНЕРГОЗБЕРЕЖЕННЯ В МОБІЛЬНИХ СЕНСОРНИХ МЕРЕЖАХ

Бондарець Я.Б., Лисенко О.І.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: yar.bondarets@gmail.com

Development of energy saving methods in mobile sensor networks

This article describes the problem of saving energy in mobile sensor networks. Mobile sensor networks are increasingly being used to monitor environmental parameters, control structures in war zones. Sensors are often placed in hard-to-reach places, so one of the most important requirements for a wireless sensor network is its autonomy. The lifetime of a node is limited by the lifetime of the power source. The solution to this issue directly affects the development of a wireless sensor network.

Мобільні сенсорні мережі представляють собою сукупність малопотужних, відносно недорогих і компактних приладів, частина з яких забезпечена сенсорами або іншими джерелами інформації, які включені в деяке фізичне оточення і об'єднанні за допомогою радіоканалу. Область покриття таких мереж може складати від декількох квадратних метрів до декількох квадратних кілометрів за рахунок можливості ретрансляції повідомлень від одного елементу мережі до іншого.

З розвитком технологій мобільні сенсорні мережі все частіше використовуються для моніторингу різних типів даних: в системах безпеки, контролю конструкцій, параметрів навколишнього середовища, для відслідковування цілей під час бойових дій. В подібних системах такі дані фіксуються мультисенсорами, які входять в склад вузлів, що розташовуються в необхідних для моніторингу точках. Ці дані передаються по мобільній мережі в центральний вузол для обробки і подальшого прийняття рішення.

Так як сенсори часто розташовують у важкодоступних місцях одним з головних вимог до бездротової сенсорної мережі (БСМ) є їх автономність, виконати яке можна, зменшивши енергоспоживання кожного вузла. Час життя вузла БСМ обмежена часом життя джерела живлення, і завдання зниження споживання енергії як ніколи стає важливою, а ефективність її

рішення безпосередньо впливає на подальший розвиток безпроводових сенсорних мереж.

Найбільш енергозатратним компонентом зазвичай є радіо-модуль. Для скорочення енергетичного розсіювання при бездротовому зв'язку застосовується оптимізація радіо-параметрів, таких як система кодування, напрям антени, передача електроенергії та спосіб модуляції. Наприклад, енергетичне виснаження викликається споживана потужність схеми і споживана потужність сигналу, що передається. Для коротких відстаней споживання схеми більше, ніж потужність передачі в той час як для довше розташовується потужність сигналу стає домінуючою. Існуюче дослідження намагається знайти хороший компроміс між розміром сукупності (кількість символів використовується), швидкість передачі інформації (кількість інформаційні біти на символ), час передачі, відстань між вузлами і шумом.

Іншим підходом до зменшення енергоспоживання сенсорів є використання направлених антен. Направлені антени дозволяють сигналам бути відправленими та отриманими в одному напрямку за один раз, що покращує передавальний діапазон і пропускну здатність. Направлені антени можуть вимагати, щоб методи локалізації були орієнтовані, але мультисв'язки може виникати в безпосередній близькості, що призводить до простого повторного використання пропускну здатності. На відмінну від всенаправлених датчиків, які передають в небажаних напрямках, підслуховуюча межа направлених антен і для даного діапазону, вимагає меншого кількості живлення. Таким чином, вони можуть покращити пропускну здатність мережі та час життя при впливі задержки і можливість об'єднання.

Іншим підходом для зменшення енергоспоживання це зменшення обсягу даних, який буде відправлений на прийом. Два способи можуть бути прийняті спільно: обмеження непотрібних даних та обмеження упізнаних даних, тому що передача даних і прийом є дорогими з точки зору споживання енергії.

Коли датчики надмірно розміщені для забезпечення хорошого покриття простору мережі, можливо деактивувати деякі вузли зберігаючи

при цьому з'єднання та всі мережеві операції. Протоколи управління топологією використовують резервування для динамічної адаптації топології мережі на основі потреб програми, щоб мінімізувати кількість активних вузлів.

Дійсно, вузли, які не потрібні для забезпечення можливості з'єднання або покриття, можуть бути вимкнені для продовження часу життя мережі, як показано на рисунку 1. Пропонуються рішення, здатні до підтримки мережевого покриття при зменшенні споживання енергії мережі шляхом активації тільки підмножини вузлів, з мінімальною областю перекриття. Також розглядається проблема вибору підмножини активних підключені датчики для корельованого збору даних. Це дуже корисно в додатках таких як, моніторинг середовища, де дані залежать від місця розташування, оскільки дані неактивних вузлів можна вивести з активних вузлів через просторову кореляцію.



Рис. 1. Приклад методу контролю топології який застосовуються в мережі. Для покриття повного поля , датчик повинен бути активним в кожній області мережі.

Література

1. Razzaque M. A., Bleakley, C., Dobson, S. Compression in wireless sensor networks: A survey and comparative evaluation. ACM Transactions on Sensor Networks (TOSN), 2013. – Vol. 10, No. 1, Article 5.
2. Агафонов Н. Технологии беспроводной передачи данных, «Беспроводные технологии» №1, 2014 г.
3. C.Siva Ram Murthy, B.S.Manoj —Ad Hoc Wireless Networks: Architectures and Protocols, Prentice Hall, 2004, 880p.

ФИЛЬТРАЦИЯ ПАРАМЕТРОВ ДВИЖЕНИЯ ИСТОЧНИКА РАДИОИЗЛУЧЕНИЯ НА ОСНОВЕ УГЛОМЕРНЫХ ИЗМЕРЕНИЙ СЕНСОРНОЙ СЕТИ

Товкач И.О., Жук С.Я.

КПИ им. Игоря Сикорского, г. Киев, Украина

E-mail: tovkach.igor@gmail.com

Filtering of radio source movement parameters on the basis angle of arrival measurements of the sensor network

Using the mathematical apparatus of Kalman filter, the recurrent algorithm has been developed for estimating the radio source movement parameters based on AOA-measurements of sensor network. Analysis of the developed algorithm executed using statistical modeling.

Последние достижения в области беспроводных сенсорных сетей (БСС) открывают новые возможности при решении задачи определения местоположения источников радиоизлучения (ИРИ). БСС позволяют создавать локальные системы позиционирования, которые находят применение при мониторинге окружающего пространства, ликвидации последствий стихийных бедствий, в интеллектуальных транспортных и охранных системах. В течение последних лет был разработан ряд методов для определения местоположения неизвестного ИРИ с помощью БСС [1,2]: RSS (Received Signal Strength), ToA (Time of Arrival), TDoA (Time Difference of Arrival), AoA (Angle of Arrival). Одним из перспективных методов определения координат неизвестного ИРИ с использованием БСС является AoA метод на основе технологии MIMO [3].

AoA метод основан на определении местоположения ИРИ, как точки пересечения линий положения, соответствующих измеренным в двух разнесенных точках приема пеленгам. Достоинством данного метода является его простота. Поэтому он нашел самое широкое применение на практике.

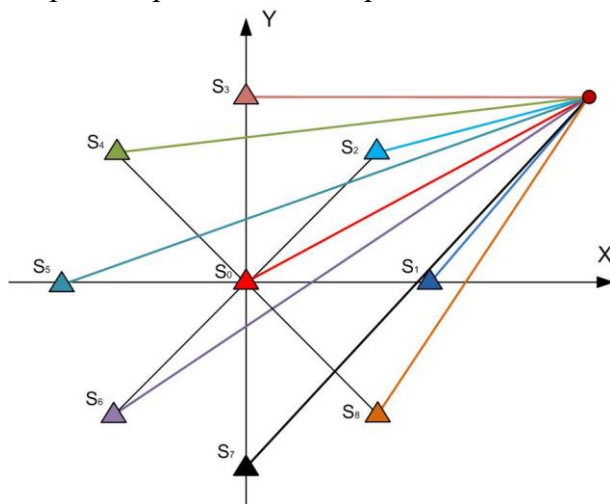


Рис. 1. Конфигурация сенсорной сети из девяти датчиков.

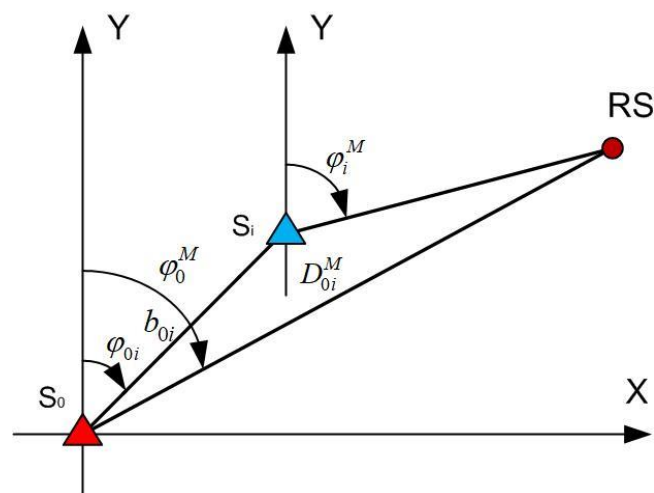


Рис. 2 Измерения азимутов ИРИ 0-м и i -м датчиками сенсорной сети.

БСС состоит из набора датчиков с координатами (x_j^s, y_j^s) , $j = \overline{0, n}$. На рис. 1 показаны структурная схема сенсорной сети на плоскости, состоящей из девяти датчиков. Положение ИРИ характеризуется точкой с координатами (x, y) . Для определения

положения ИРИ используются пары датчиков $S_0 S_i$, $i = \overline{1, n}$. В качестве опорного для всех пар применяется датчик S_0 . При использовании метода АОА в одном цикле измерения все датчики измеряют пеленги ИРИ φ_i^M , $i = \overline{0, n}$ с одинаковой дисперсией ошибок измерений пеленгов σ^2 $i = \overline{0, n}$.

Расстояние от опорного приемника S_0 до цели находится с помощью измеренных 0-м и i -м датчиками пеленгов ИРИ φ_i^M и φ_0^M . По теореме синусов:

$$D_{0i}^M = \frac{b_{0i} \sin(180 - (\varphi_{0i} - \varphi_i^M))}{\sin((\varphi_{0i} - \varphi_i^M) - (\varphi_{0i} - \varphi_0^M))}, \quad (1)$$

где φ_{0i} – азимут i -ой базы; b_{0i} – длина i -ой базы.

Координаты ИРИ в прямоугольной системе координат на основе рассчитанного значения дальности D_{0i}^M и измеренного опорным датчиком азимута φ_0^M определяются по формулам:

$$x_{0i}^M = D_{0i}^M \sin \varphi_{0i}^M; \quad (2)$$

$$y_{0i}^M = D_{0i}^M \cos \varphi_{0i}^M. \quad (3)$$

Повышение точности определения местоположения ИРИ может быть достигнуто путем траекторной фильтрации. Необходимо на основе математического аппарата калмановской фильтрации синтезировать алгоритм оценивания параметров движения ИРИ на основе АОА-измерений сенсорной сети.

Движение ИРИ в прямоугольной системе координат описывается стохастической динамической системой вида [4]:

$$u(k) = Fu(k-1) + G\omega(k), \quad (3)$$

где $u(k)$ – вектор состояния, включающий параметры движения ИРИ по осям прямоугольной системы координат.

Выполняя линеаризацию уравнений (2,3), можно получить рекуррентный алгоритм оценивания вектора состояния u_k , в виде фильтра Калмана [4]

$$K_k = \hat{P}_{k-1} \cdot H \left[H \hat{P}_{k-1} H + R_k \right]^{-1}; \quad (4)$$

$$\hat{u}_k = \hat{u}_{k-1} + K_k \left[Y_k - H \hat{u}_{k-1} \right]; \quad (5)$$

$$\hat{P}_k = \hat{P}_{k-1} - K_k H \hat{P}_{k-1}, \quad (6)$$

где $\hat{u}_k$ – оценка вектора состояния u_k на k -м шаге; $\hat{P}_k$ – корреляционная матрица ошибки оценки вектора состояния u_k на k -м шаге; $Y_k = (x_{0i}^M, x_{0i}^M)^T$ – вектор измерения; K_k – коэффициент усиления фильтра; H – матрица наблюдения, R_k – корреляционная матрица, имеют вид

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}, \quad R_k = \begin{bmatrix} \sigma_{0iX}^2 & \sigma_{0iXY}^2 \\ \sigma_{0iXY}^2 & \sigma_{0iY}^2 \end{bmatrix}.$$

Анализ эффективности разработанного алгоритма проведен с помощью статистического моделирования. При этом сенсорная сеть (рис. 1) состоит из девяти датчиков, располагающихся на окружности с радиусом 100 м. Для наглядности работы алгоритмов была сформирована тестовая траектория движения ИРИ в виде окружности с

радиусом 1000 м относительно опорного датчика S_0 . СКО ошибок измерений $\sigma = 0.4^\circ$. Темп поступления информации $T=1$ с. Испытания проводились по ста реализациям.

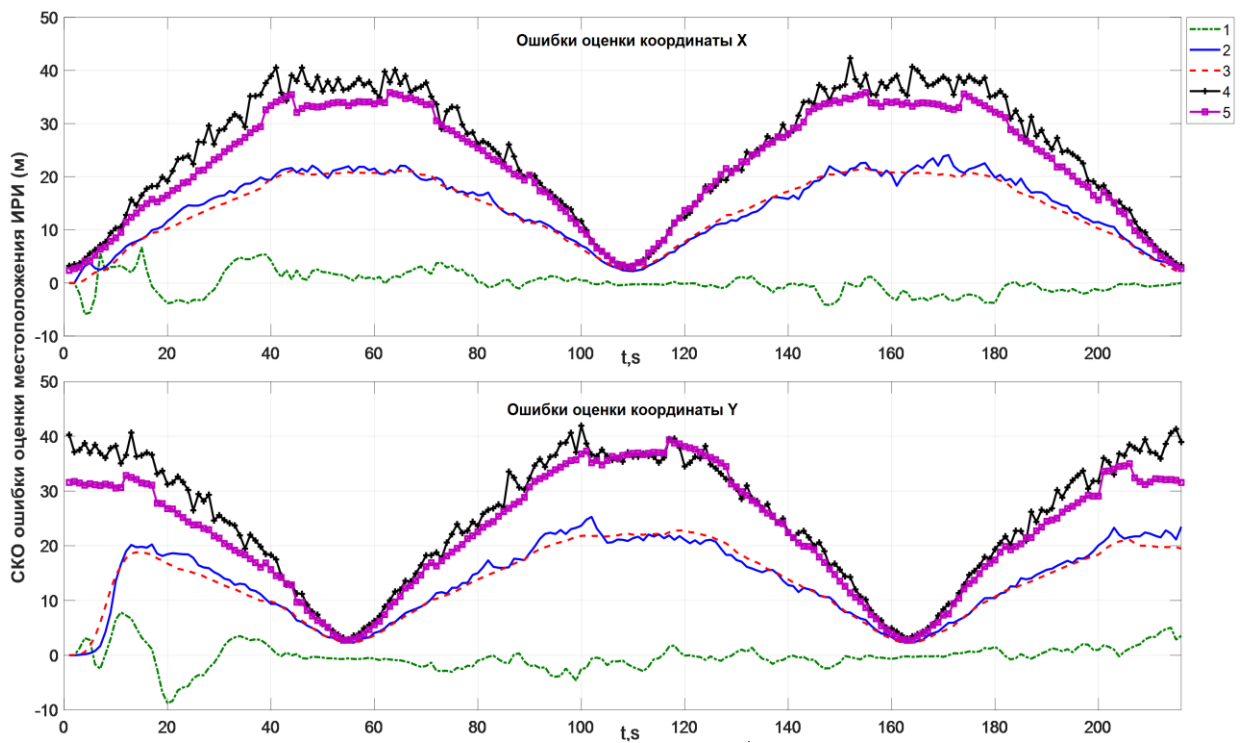


Рис. 3. СКО ошибки оценки местоположения цели для пары датчиков сенсорной сети.

На рис. 3 показаны полученные методом Монте-Карло зависимости математических ожиданий (кривые 1) и СКО (кривые 2) ошибок оценки местоположения БПЛА по координатам X , Y , а также СКО (кривые 3) ошибок оценки, рассчитанных разработанным фильтром. Также на рис. 3 показаны зависимости СКО ошибок оценки местоположения ИРИ, которое соответствует рекуррентному методу определения местоположения (кривые 4,5). Применение траекторной фильтрации позволяет уменьшить СКО ошибки определения местоположения ИРИ в 1.5-2 раза.

Литература

1. Zhang, Weile & Yin, Qinye & Chen, Hongyang & Gao, Feifei & Ansari, Nirwan., "Distributed Angle Estimation for Localization in Wireless Sensor Networks". IEEE Transactions on Wireless Communications. 12, 2012, 527-537. 10.1109/TWC.2012.121412.111346.
2. Товкач И. О. Рекуррентный алгоритм пассивной локации в сенсорной сети на основе измерения мощности принимаемого сигнала / И.О. Товкач, С.Я. Жук // Вестник НТУУ «КПИ». Серия Радиотехника. Радиоаппаратостроение. – 2016. – № 66. – с. 46-55
3. Amiri, Rouhollah & Zamani, Hojatollah & Behnia, Fereidoon & Marvasti, Farokh., "Sparsity-aware target localization using TDOA/AOA measurements in distributed MIMO radars", ICT Express. 2, 2016. 10.1016/j.icte.2016.02.002.
4. Жук С.Я. Методи адаптивного оцінювання параметрів руху безпілотного літального апарату на основі вимірювань сенсорної мережі : монографія / С.Я. Жук, І.О. Товкач. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2019, – 172 с.

СПОСОБЫ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ СБОРА ДАННЫХ МОНИТОРИНГА С ИСПОЛЬЗОВАНИЕМ БПЛА ПРИ КЛАСТЕРИЗАЦИИ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ

Романюк В.А.¹ Лысенко А.И.², Романюк А.В.², Жук А.В.¹

¹Военный институт телекоммуникаций и информатизации, Украина

²Институт телекоммуникационных систем КПИ им. Игоря Сикорского

E-mail: romval2016@gmail.com

Methods for increasing the efficiency of collecting UAV monitoring data in clustering wireless sensors networks

Methods for increasing the lifetime of wireless sensor networks with clustering by reducing and redistributing the battery power consumption of nodes at all stages of network's operation, ways to reduce the time of acquisition of UAV monitoring data by optimizing its positioning are proposed.

Беспроводные сенсорные сети (БСС) получают широкое применение в промышленности, сельском хозяйстве, условиях чрезвычайных ситуаций, на поле боя и т.п. Площадь мониторинга БСС может составлять от нескольких метров до десятков километров. Для БСС большой размерности при отсутствии телекоммуникационной инфраструктуры целесообразно использование БПЛА (или сеть БПЛА) в качестве воздушного шлюза для сбора данных мониторинга.

Для реализации процесса сбора данных мониторинга БПЛА от сенсорных узлов в системе управления БСС необходимо реализовать соответствующие методы и алгоритмы. Для повышения эффективности процесса сбора данных в БСС проводится ее кластеризация, выделяются главные узлы кластеров, собирающие данные мониторинга в кластере и передающие эти данные на БПЛА при его полете. Предложенные на сегодня методы сбора данных с узлов сенсорных сетей с использованием БПЛА не учитывают требования различных целевых функций управления, особенности функционирования конкретных сетей и требуют дальнейшего совершенствования.

Целью работы является анализ и рассмотрение способов повышения эффективности процесса сбора данных с сенсорных узлов БСС с использованием БПЛА при ее кластеризации.

Целевыми функциями управления при сборе данных могут быть [1]:

1. Максимизация или обеспечение заданного времени функционирования БСС ($\max T_{\text{ф}}$ или $T_{\text{ф}} \geq T_{\text{фзад}}$) при заданных ограничениях на время $T_{\text{сб}}$ и объемы $V_{\text{дм}}$ собираемых данных мониторинга, количество имеющихся для использования БПЛА – $N_{\text{зад}}$.

Данная целевая функция достигается уменьшением расхода энергии узлами БСС следующими способами (рис. 1):

- уменьшение мощности передачи между двумя сенсорными узлами;
- уменьшение расстояния и, соответственно, уменьшение мощности передачи и затраченной энергии между головными узлами кластеров и БпЛА, что позволяет увеличивать скорость передачи данных (например, для протокола IEEE 802.11);
- перераспределение расхода энергии между узлами за счет реализации соответствующих алгоритмов управления сетью – алгоритмов покрытия (разбиение на независимые множества покрывающих узлов и составление графиков мониторинга по множествам), алгоритмов построения и поддержания топологии и маршрутов передачи данных в кластерах [2], алгоритмов выбора главных узлов в кластере (за счет использования энергозависимых метрик);
- уменьшение объема служебного трафика при реализации алгоритмов управления на всех уровнях OSI (например, за счет введения кросс-уровня);
- уменьшение вычислительной сложности алгоритмов управления сетью.

Кроме этого, уменьшение расхода энергии сенсорными узлами в кластере может быть достигнуто за счет:

- сокращения времени пребывания узлов в активном состоянии или увеличение режима сна;
- уменьшения радиуса мониторинга узлом или площади мониторинга сетью (формирование α -покрытия);
- создания избыточного количества узлов, необходимых для покрытия заданной площади (объекта);
- агрегации передаваемых данных мониторинга от простых узлов главному.

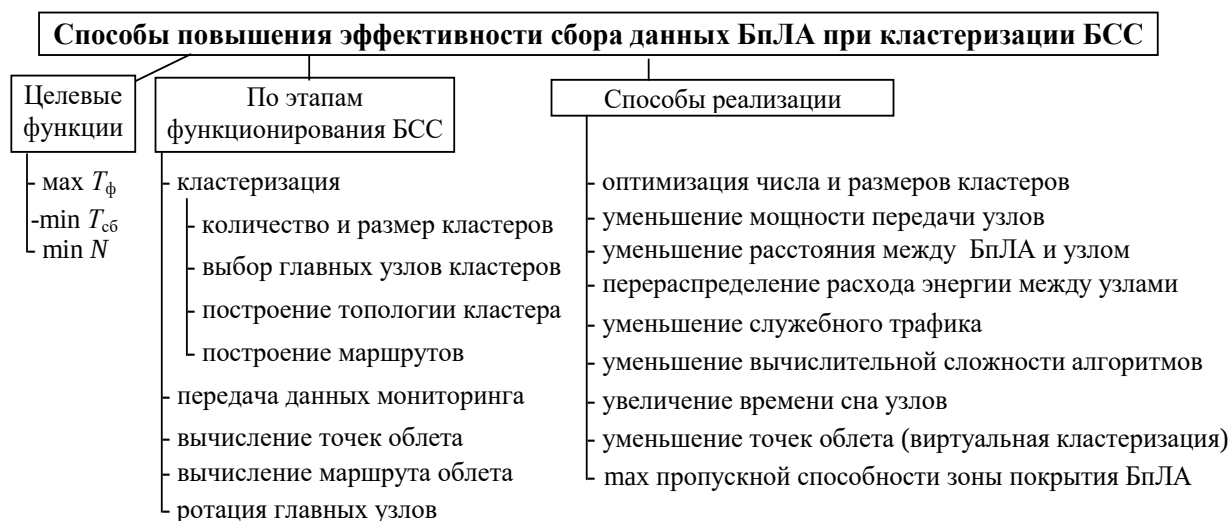


Рис. 1. Способы повышения эффективности сбора данных мониторинга.

2. Минимизация или обеспечение заданного времени сбора данных ($\min T_{\text{сб}}$ или $T_{\text{сб}} \leq T_{\text{сбзад}}$) при ограничениях на количество БПЛА $N \leq N_{\text{зад}}$, заданный объем данных мониторинга $V_{\text{дм}} \leq V_{\text{дмзад}}$ и время функционирования сети

$$T_{\text{ф}} \leq T_{\text{фзад}}.$$

Время сбора данных зависит от длительности маршрута полета (зависит от количества кластеров, местоположения их главных узлов, назначенных точек обмена с БПЛА), скорости полета БПЛА, скорости обмена данными между главными узлами и БПЛА (кроме прочего зависит от расстояния между ними).

3. Минимизация количества БПЛА ($\min N$), необходимых для сбора данных с заданным качеством, при ограничениях на время сбора информации $T_{\text{сб}} \leq T_{\text{сбзад}}$, объем собираемых данных мониторинга $V_{\text{дм}} \leq V_{\text{дмзад}}$ и время функционирования сети $T_{\text{ф}} \leq T_{\text{фзад}}$.

Достигается разделением БСС на подсети и оптимизацией процесса сбора данных в каждой подсети.

Реализация целевых функций управления БСС должна достигаться на различных этапах функционирования сети (рис. 1):

1. Кластеризация сети.

а) Расчет количества, размеров кластеров и периода ротации главных узлов. Оптимизация данных параметров должна обеспечить реализацию целевых функций управления. Их значения определяются размерностью БСС, площадью покрытия, характеристиками сенсорных узлов и БПЛА и принятыми алгоритмами управления.

Меньшее число кластеров приводит к меньшему количеству главных узлов, меньшей длине маршрута полета БПЛА и уменьшает время облета (сбора данных). Однако это увеличивает диаметр кластеров и, соответственно, увеличивает время на их организацию. Кроме этого, увеличивается расход энергии узлов на служебный трафик, передача данных от простых узлов к главным осуществляется по более длинным маршрутам. Для расчета времени функционирования БСС предложена аналитическая модель, учитывающая расход потребления энергии узлов в зависимости от его функций (только мониторинг, мониторинг плюс маршрутизация, мониторинг плюс главный узел кластера) и объема данных мониторинга, от заданного времени функционирования сети (или количества раундов сбора

данных БпЛА) [1].

б) Формирование кластеров. Осуществляется путем обмена служебными сообщениями между узлами с реализацией соответствующих алгоритмов выбора главных узлов кластеров с учетом приоритета целевых функций управления сетью. Алгоритм выбора главного узла должен учитывать свертку метрик: энергия батареи узла кластера, уровень сигнала в радиоканале узел-БпЛА, расположение в кластере (в центре или на краях) (рис. 2) и т.п.

в) Построение топологии кластера. Должно осуществляться по заданным целевым функциям управления сетью (например, для минимизации расхода энергии узлов – построение энергоэффективной топологии [3], минимизация времени передачи – построение топологии с малым диаметром и т.п.).

г) Построение и поддержка маршрутов в кластере от простых узлов к главным по свертке метрик, учитывающих также целевые функции управления: мощность передачи, энергия батарей узлов, пропускная способность и другие.

2. Передача данных мониторингу в кластерах от простых узлов к главным узлам с заданным качеством по определенным ранее маршрутам.

3. Нахождение положения в пространстве БпЛА (точек сбора данных мониторинга, в простейшем случае главный узел – точка сбора).

Для минимизации времени сбора осуществляется поиск минимального количества точек (положений БпЛА) сбора данных. Для этого осуществляется виртуальная кластеризация головных узлов [1], например, с использованием алгоритма FOREL (FORmal ELeMent) с адаптацией размера зоны покрытия БпЛА R (для уменьшения расстояния между главными узлами и БпЛА) рис. 2.

Для максимизации пропускной способности между главными узлами кластеров и БпЛА в зоне его покрытия предлагается вычислять его положение в зависимости от их нагрузки, используя соответствующую математическую модель [3].

4. Построение кратчайшего маршрута для облета точек сбора (целевая функция – минимум времени сбора данных).

5. Полет БпЛА по рассчитанному маршруту и сбор данных. Для этого высота (расстояние между БпЛА и главным узлом устанавливается для

обеспечения заданной скорости передач данных) и скорость полета рассчитываются для обеспечения времени, достаточного для обеспечения качества передачи всех данных мониторинга.

Уровень мощности передачи между БПЛА и главным узлом поддерживается на минимальном уровне.

5. Ротация главных узлов кластеров. Осуществляется выбор новых главных узлов кластера, перестроение топологии кластеров, маршрутов передачи, точек сбора и маршрутов полета.

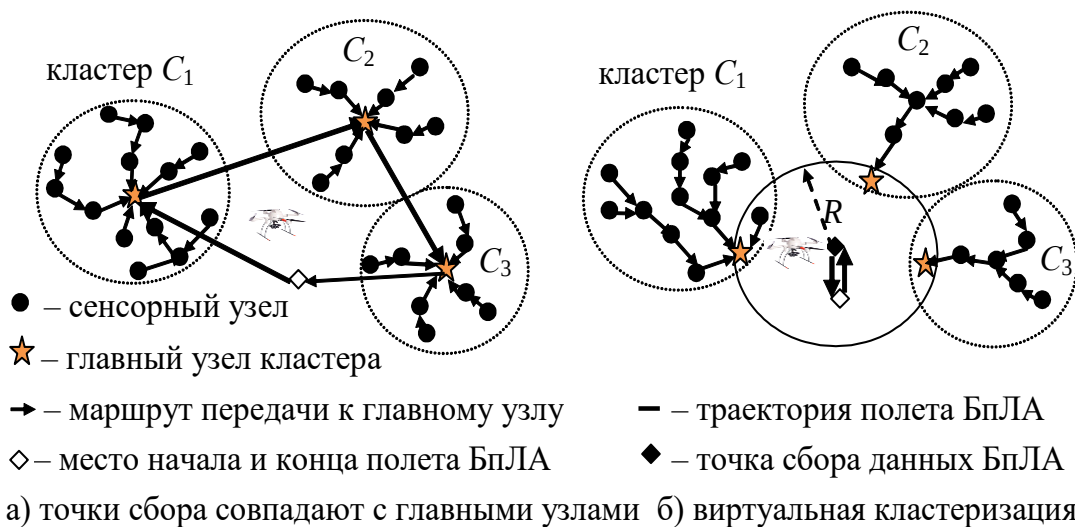


Рис. 2. Варианты облета БПЛА при различном размещении точек сбора данных.

Проведенное моделирование предложенных способов управления сетью показано эффективность их реализации. Для БСС размерностью 100, 150, 200 узлов увеличение времени функционирования сети составило до 20%, сокращение времени сбора данных – до 50%.

Література

1. Романюк А.В. Алгоритм временной кластеризации узлов беспроводных сенсорных сетей для сбора информации мониторинга с использованием БПЛА. Научно-технічний збірник «Адаптивні системи автоматичного управління». № 2 (33). 2018. С. 106 – 117.
2. Жук О.В. Романюк А.В., Сова О.Я., Ткаченко Д.В. Управління топологією в безпроводних сенсорних мережах. Збірник наукових праць ВІПІ. 2018. №1. С. 90 – 99.
3. Степаненко Э.О. Модель позиціонування телекомунікаційної аероплатформи для оптимізації пропускної здатності вузлів зони покриття. Збірник наукових праць ВІПІ. 2019. №1. С. 97 – 104.

ДОСЛІДЖЕННЯ ЗАВАДОСТІЙКОСТІ ТЕХНОЛОГІЇ LORAWAN

Міночкін Д.А., Рибак О.О.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: alex96.rybak@gmail.com

Research of interference noise immunity technology LoRaWAN

LoRaWAN is a promising low-power network technology (LPWAN). LoRaWAN is one technology that are less susceptible to noise and interference than other LPWAN protocols. This technology operates in the unlicensed range, which increases the chances of interference in the communication line.

LoRaWAN [1], складається з кінцевих вузлів, шлюзів, мережевих серверів і додатків. LoRaWAN є одним із популярних протоколів в LPWAN. LoRaWAN має шість ортогональних коефіцієнтів передачі (SF) даних [2] для поліпшення пропускної здатності каналу і ефективності використання спектру. Ортогональність дозволяє здійснювати зв'язок з різними SF на одному і тому ж каналі. Вибір SF залежить від дальності зв'язку і тривалості повідомлення. Моделювання та емпіричні експерименти з точки зору між мережевими перешкодами LoRaWAN вивчені в [3, 4], відповідно вони роблять висновок, що завади погіршують продуктивність мережі LoRaWAN [3].

Метод модуляції LoRaWAN запатентована Semtech [5-7], заснований на технології з розширеним спектром з використанням лінійної частотної модуляції (ЛЧМ / CSS) з інтеграцією прямого виправлення помилок (FEC) [5]. Це рішення значно підвищує чутливість приймача і робить приймач, стійким до відхилення частот від номінального значення. Технологія LoRaWAN дозволяє демодулювати сигнали на рівні -19 дБ по відношенню до рівня сигнал/шум, а частотна маніпуляція (FSK) системи, можуть коректно працювати з сигналами на рівні, не нижче, ніж 8-10 дБ вище рівня шуму. Через свою високу чутливість (-146 дБм) LoRaWAN ідеально підходить для пристроїв з вимогами низького енергоспоживання і високої стабільності зв'язку на великі відстані.

Кінцевий вузол передає пакети по призначеному каналу (ам) висхідної лінії зв'язку, і кілька шлюзів прослуховують прийом пакетів. Кожен шлюз надсилає прийняті пакети на призначений мережевий сервер, тому мережевий сервер може мати одну або кілька копій одного пакета. Потім мережевий сервер пересилає отримані пакети на відповідний сервер додатків. Для кожного отриманого пакету мережевий сервер пересилає його тільки один раз і видаляє дублікати, якщо отримано кілька копій. Мережевий сервер також відповідає за вибір правильного шлюзу для подальшої передачі по низхідній лінії зв'язку, якщо у мережевого серверу є очікуваний пакет (и), який повинен бути відправлений на кінцевий вузол.

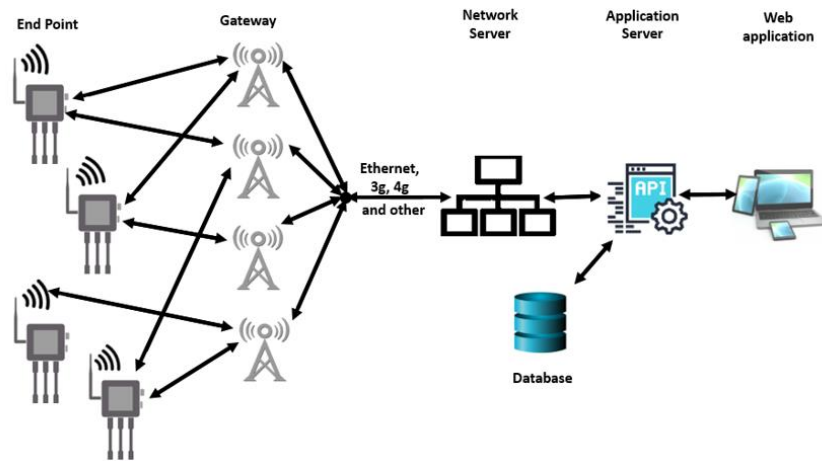


Рис. 1. Топологія мережі LoRaWAN.

Налаштування LoRaWAN чипу включає в себе налаштування параметрів SF, BW і швидкості кодування (CR). Вони використовуються для визначення еквівалентного бітрейта і періоду часу в ефірі. Швидкість передачі даних LoRaWAN може бути отримана з параметрів SF і BW. Швидкість кодування є параметром для прямого виправлення помилок. Більш низька швидкість кодування забезпечує кращий захист пакетів, щоб максимізувати термін служби акумулятора кінцевих вузлів, так і загальну ємність мережі. Мережева інфраструктура управляє швидкістю передачі даних і вихідною РЧ-потужністю для кожного кінцевого вузла індивідуально за допомогою схеми адаптивної швидкості передачі даних (ADR). Потім кінцевий вузол може передавати дані по доступному каналу в будь-який момент часу, використовуючи відповідну швидкість передачі даних при обмеженнях застосування псевдо випадковим перемиканням каналів для кожної передачі з дотриманням максимального робочого циклу. Тому для підтвердження високої завадо захищеності технології LoRaWAN було проаналізовано такий експеримент.

Генератор SMA100 (R&S), забезпечує модуляцію сигналу в широкому діапазоні в якості джерела завад. Адитивна суміш вихідних сигналів передавача LoRaWAN і завад подається на вхід приймача LoRaWAN. Рівень сигналів та завад вимірюють за допомогою спектра аналізатора FSQ26 (R&S) [6].

Умови вимірювання обрані таким чином:

- вимірювання в смузі $BW = 125$ кГц;
- потужність сигналу = -68 дБм
- потужність перешкоди = -46 ... - 52 дБм.

Результати вимірювань показані на рисунку 2.

1. Ефект широкосмугових перешкод (шум).

2. Вплив вузько смугових перешкод. Перешкода на частоті = 868,150 МГц.

3. Вплив гармонійної перешкоди. Перешкода на частоті = 868,150 МГц.

Порогові значення модуляції LoRaWAN відображається в характеристиках завадостійкості – лінійної частотної модуляції [8].

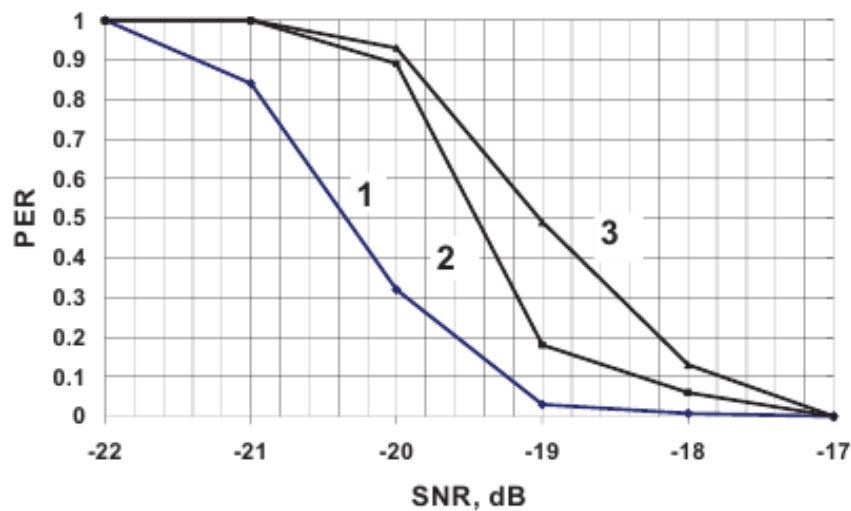


Рис. 2. Завадостійкість LoRaWAN.

Коли відношення сигнал/шум (SNR), більше, ніж -17 дБ, то значення PER дорівнює 0. Якщо сигнал/шум менше ніж -21 дБ, то значення PER прагне до одиниці для всіх перешкод. В середині інтервалу -17 ... -21 дБ, є різниця в PER. Ця особливість завадостійкості (порогові явища) істотно обмежує спектр системи радіозв'язку з LoRaWAN, так як він вимагає значного запасу для SNR для забезпечення стабільного прийому повідомлень на максимальній дальності.

Висновок. Стандарт LoRaWAN має високу завадостійкість, при прийомі сигналів в умовах певних завад. Був представлений вплив завад на прийомі сигналів з модуляцією LoRaWAN. Результатом оцінки завадостійкості практично збігається з тими, значеннями, що заявлено розробником технології: в 0 з SNR = -19 дБ (на SF = 12), Однак вже при SNR = -21 дБ, прийом помилок пакетів PER наближається до 1.

Література

1. N. Sornin, M. Luis, T. Eirich, T. Kramp, and O. Hersent, "LoRaWAN Specification," LoRa Alliance Inc., San Ramon, CA, Ver. 1.0.2, Jul. 2016.
2. A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," IEEE Communications Surveys & Tutorials, vol. 11, no. 4, pp. 42–56, Fourth Quarter 2009.
3. T. Voigt et al., "Mitigating inter-network interference in LoRa network-s," [Online]. Available: <https://arxiv.org/abs/1611.00688>.
4. K. Mikhaylov et al., "On LoRaWAN scalability: Empirical evaluation of susceptibility to inter-network interference" in press.
5. J. Haxhibeqiri, E. Poorter, I. Moerman, J. Hoebeke. "A Survey of LoRaWAN for IoT: From Technology to Application." Sensors, vol. 18, pp. 2-38, Nov. 2018.
6. K. Staniec, M. Kowal. "LoRa Performance under Variable Interference and Heavy-Multipath Conditions." Wireless Communications and Mobile Computing, vol. 2018, Article ID 6931083, Apr. 2018.
7. P. Robyns, P. Quax, W. Lamotte, W. Thenaers. "A multi-channel software decoder for the LoRa modulation scheme," in Proc. IoT BDS, 2018, pp. 41-51.
8. D. Singh, O. Aliu, M. Kretschmer. "LoRa Wan Evaluation for IoT Communications," in Proc. ICACCI, 2018, pp. 163-171.

АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ НА ОСНОВІ ТЕХНОЛОГІЇ БЛОКЧЕЙН В СФЕРІ ТЕЛЕКОМУНІКАЦІЙ

Міночкін Д.А., Юдін М.М., Малецький Л.В.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: misha.yudin19@gmail.com

The analysis of existing solutions on the basis of Blockchain technology in the field of the Telecommunications

Blockchain is currently one of the most talked-about technologies. Today it is already used in many fields of life - from crypto currencies (which popularized the technology in first place) to electronic document management in government sectors. The potential of the technology makes it possible to improve the performance of some branches of the telecommunications industry. IBM has already introduced the IBM Blockchain Platform technology, which manages authentication and billing processes of roaming subscribers. The mobile operators AT&T, T-Mobile, Verizon and Asia Pacific Telecom are already using blockchain technology in telecommunications. Blockchain can also be used in other fields of telecommunications. For this reason, it makes sense to analyze which companies are using blockchain and how they are using it.

Поняття блокчейн. Блокчейн – це публічна електронна книга, що базується на технології Peer-2-Peer (P2P), тобто яка відкрито поширюється між користувачами для отримання незмінного ланцюгу записів, кожен запис у якому має свою відмітку часу та пов'язаний з попереднім записом технологією хешування. Кожен запис називається блоком (block), а сама книга називається ланцюгом (chain), що і утворює назву технології. [1]

Поняття смарт контракту. Смарт контракт – електронна версія договору (контракту) що сама виконує умови описані в договорі. Це додаток блокчейну який автоматично виконується при підписанні транзакції (тобто створенні нового блоку в ланцюгу), або при інших умовах, що закладені в смарт контракті (наприклад, певна кількість годин після підписання смарт контракту). Умови договору та умови виконання смарт контракту формуються в процесі створення смарт контракту та стають незмінними після приєднання до блокчейну (якщо відсутня умова ануляції контракту, що прописана в смарт контракті). [2]

Принцип роботи блокчейну та смарт контрактів в мобільному зв'язку. Розглянемо принцип роботи технологій блокчейну та смарт контрактів в роумінгу на основі технології IBM Blockchain Platform 2.0 (IBPv2).

(1) - домашній оператор (див. рис.), створює смарт контракти та додає їх до загальної бази даних (блокчейну). Умовами цих смарт контрактів можуть бути: списання коштів за вхідний або вихідний дзвінок, списання коштів за використання передачі даних та мультимедіа послуги, тощо.



Рисунок 1. схема роботи IPv2 [3].

(2) - клієнт роумінгу (див. рис.), підписує ці смарт контракти у момент активації SIM картки в мережі оператора-партнера роумінгу. Якщо передплачені послуги, які входять у тариф клієнта, досягають ліміту – оператор, що надає послуги, зв’язується з таким клієнтом та пропонує новий оверлімітний тариф. Якщо клієнт погодився на оверлімітний тариф – він стає (3) клієнтом з оверлімітом.

(4) - партнер роумінгу (див. рис.), реєструє всі послуги які використовують клієнти та підписує смарт контракти, створені домашнім оператором, що призводить до списання коштів за послуги з клієнтів.

(5) - якщо хтось намагається аутентифікуватись у мережі за допомогою підробленої SIM картки (див. рис.), система виявляє це і позначає цю особу шахраєм та відмовляє цій особі в обслуговуванні [3].

Телекомунікаційні компанії, що використовують технології блокчейн та смарт контракт. Велика кількість телекомунікаційних компаній використовують технології блокчейн та смарт контрактів. Список таких компаній та для чого вони використовують технологію блокчейн:

- AT&T використовує технологію блокчейн в сфері ремонту телефонних апаратів абонентів – для забезпечення оригінальності запчастин, що використовуються; [4]
- T-Mobile використовує блокчейн в своєму проєкті NEXT Identity platform – як базу даних клієнтів; [4][5]
- Verizon запатентував технологію віртуальних SIM карток vSIM, що базуються на блокчейні; [5]
- Comcast готується запустити платформу Blockgraph – технологію яка базується на блокчейні і дає змогу рекламодавцям отримувати загальну статистику про глядачів кабельного ТБ без розкриття особистості; [5]

- Carrier Blockchain Study Group анонсували, що Тайванський оператор мобільного зв'язку Asia Pacific Telecom та не названий оператор із США використали їх платформу для роумінгової оплати послуг користувачами. [6]
- Bubbletone – децентралізований оператор мобільного зв'язку, що спирається на надання послуг роумінгового зв'язку. [7]

Висновок. Технологія блокчейн являє собою доволі перспективну та розвинуту технологію. Блокчейн та смарт контракти вже використовуються багатьма компаніями в сфері телекомунікацій. Вже є розробки компанії IBM, які керують процесами аутентифікації та білінгу абонентів мобільних операторів в роумінгу. Це означає, що впровадження технології блокчейн та смарт контрактів в інші сфери телекомунікацій, таких як: аутентифікація та білінг абонентів мереж домашніх мобільних операторів, аутентифікація абонентів приватних віртуальних мереж, білінг абонентів провайдерів кабельного телебачення, мультимедійних послуг, білінг абонентів провайдерів інтернет-послуг та інших – являє собою перспективний напрямок досліджень та розробок.

Література

1. Mearian L. What is blockchain? The complete guide [Електронний ресурс] / Lucas Mearian // ComputerWorld. – 2019. – Режим доступу до ресурсу: <https://www.computerworld.com/article/3191077/what-is-blockchain-the-complete-guide.html>
2. Dewey J. What is a Smart Contract? [Електронний ресурс] / J. Dewey, S. Amual // Bloomberg Law. – 2015. – Режим доступу до ресурсу: <https://news.bloomberglaw.com/business-and-practice/what-is-a-smart-contract/>
3. Blockchain for telecom roaming, fraud user identification, and overage management [Електронний ресурс] / [S. Nayak, A. Singh, J. Vora та ін.] // IBM. – 2018. – Режим доступу до ресурсу: <https://developer.ibm.com/patterns/blockchain-for-telecom-roaming-fraud-and-overage-management/>
4. Pirus B. How Telecom Giants AT&T And T-Mobile Are Using Blockchain [Електронний ресурс] / Benjamin Pirus // Forbes. – 2019. – Режим доступу до ресурсу: <https://www.forbes.com/sites/benjaminpirus/2019/06/13/how-telecom-giants-att-and-t-mobile-are-using-blockchain/>
5. Dalton M. The Call of Crypto: How Are Telecom Companies Using Blockchain? [Електронний ресурс] / Mike Dalton // bitrates. – 2019. – Режим доступу до ресурсу: <https://www.bitrates.com/index.php/news/p/the-call-of-crypto-how-are-telecom-companies-using-blockchain>
6. Telecoms companies complete mobile payments using blockchain [Електронний ресурс] // Ledger Insights. – 2020. – Режим доступу до ресурсу: <https://www.ledgerinsights.com/telecoms-blockchain-mobile-payments-cbsg/>
7. Which are the Top Blockchain based Decentralized Telecom Operators? [Електронний ресурс] // Krypto Graphe. – 2018. – Режим доступу до ресурсу: <https://www.kryptographe.com/decentralized-telecom-operators/>

МЕТОДИ ВИКОРИСТАННЯ BLOCKCHAIN ТЕХНОЛОГІЙ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Міночкін Д.А., Бурлака Г.Ю., Гончаренко О.М

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: fastmotion1111@gmail.com, oksanka96goncharenko@ukr.net

Methods of using blockchain technology in telecommunication systems

The fast developing Industrial Internet of Things (IIoT) technologies provide a promising opportunity to build large-scale systems to connect numerous heterogeneous devices into the Internet. Most existing IIoT infrastructures are based on a centralized architecture, which is easier for management but cannot effectively support immutable and verifiable services among multiple parties. Blockchain technology provides many desired features for large-scale IIoT infrastructures, such as decentralization, trustworthiness, trackability, and immutability. This paper presents a blockchain-based IIoT architecture to support immutable and verifiable services. However, when applying blockchain technology to the IIoT infrastructure, the required storage space posts a grant challenge to resource-constrained IIoT infrastructures.. Specially, the proposed architecture features a hierarchical storage structure where the majority of the blockchain is stored in the clouds, while the most recent blocks are stored in the overlay network of the individual IIoT networks.

У даний час більшість існуючих великомасштабних промислових IoT-інфраструктур розробляються, розгортаються і обслуговуються окремими сторонами. Як правило, вони засновані на clouds і на моделях централізованого зв'язку, у яких всі пристрої ідентифікуються, проходять перевірку автентичності і підключаються через хмарні сервери, які забезпечують великі можливості обчислень та зберігання. Поряд з швидким зростанням розмірів і складності IoT мережі, централізовані рішення IoT, однак, стають все більш дорогими через високу вартість розгортання і обслуговування, пов'язаної з мережевою та хмарною інфраструктурою. У традиційних мережах IoT дані, що надаються окремими промисловими організаціями, можуть бути ненадійними, оскільки вони можуть бути підроблені або змінені зловмисниками або власником даних. Бажано мати механізми для перевірки на достовірність даних в мережах IoT.

З огляду на ці вимоги до мереж IoT, технологія блокчейн може служити перспективним кандидатом на надання даних послуг.

Однак технологія блокчейн не може бути безпосередньо включена в існуючі рішення IoT, зважаючи на вкрай обмежені ресурси в мережах IoT і технологіях блокчейна, щоб кожен учасник повинен був зберігати точну копію блокчейна, щоб гарантувати узгодженість [1].

Пропонована архітектура розділяє інфраструктуру IoT на три рівні: локальні мережі IoT, оверлейну мережу блокчейна і хмарну інфраструктуру.

Для вирішення проблем зберігання в мережах IoT запропонована нова структура зберігання блокчейнів для ієрархічного зберігання блоків: велика частина блокчейна зберігається в хмарі, щоб використовувати його надлишкову ємність, а найновіші блоки зберігаються в оверлейну мережу окремих мереж IoT. Оскільки блоки продовжують додаватися до блокчейну, відсотковий вміст кожної частини підтримується динамічно, в основному в залежності від двох факторів: розміру поточного блокчейна і розміру сховища (наприклад, диска), що надається на узгоджених вузлах.

Технологія Blockchain має величезний потенціал у створенні надійних децентралізованих додатків IoT і надає безліч переваг з технічної точки зору. Однак технологія блокчейна все ще перебуває на ранніх стадіях, і існує безліч бар'єрів, які обмежують застосування поточної технології блокчейна до додатків IoT.

Пропонована архітектура IoT на основі ланцюжка блоків, як показано на рис. 1, складається з трьох рівнів: локальні мережі IoT, мережа blockchain P2P і clouds.

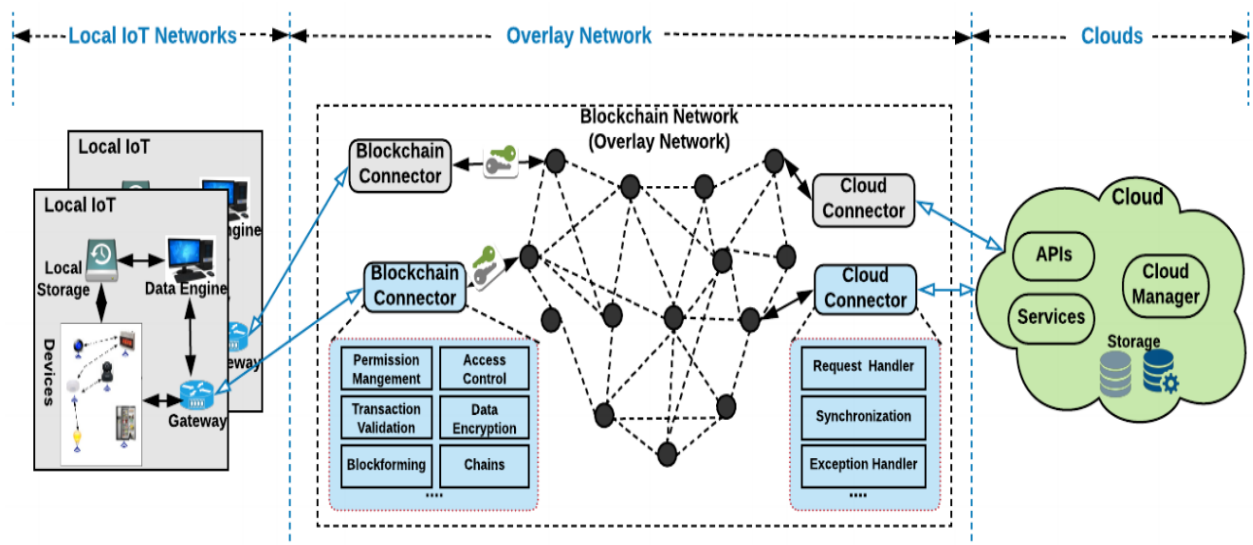


Рис. 1. Огляд архітектури IoT на основі blockchain [2].

Зверніть увагу, що запропонована архітектура IoT на основі ланцюжка блоків передбачає, що за допомогою платформи безпеки захист і передача необроблених даних в транзакції відбуваються в локальній мережі IoT. Довіра і безпека локальних транзакцій можуть бути гарантовані за допомогою платформи безпеки централізовано і приватно. І шлюз, як вузол в оверлейній мережі, відправляє підготовлені транзакції в оверлейну мережу. Після отримання транзакцій оверлейна мережа відповідає (через однорангові вузли) за створення блоків, перевірку блоків і об'єднання блоків в ланцюжок.

Запропонована архітектура пов'язує локальні мережі IoT, оверлейну мережу blockchain і Cloud інфраструктуру разом через два з'єднувача, blockchain connector і cloud connector, щоб створити ієрархічне сховище

blockchain. Blockchain connector в оверлейній мережі будує блоки в блокчейні з даних, згенерованих в мережах IoT, а cloud connector вирішує проблеми синхронізації blockchain між оверлейною мережею і cloud [3].

Перевірка транзакції і підпис даних. Механізм перевірки транзакцій специфічний для блокчейна. Як правило, транзакції перевіряються за допомогою повторного виконання вузлами, які приймають блоки. Наприклад, механізми перевірки транзакцій біткоїнів засновані на двох головних сценаріях: блокування і розблокування. Його схема перевірки головним чином заснована на моделі виведення невитрачених транзакцій (UTXO), яка визначає вихідні дані транзакції блокчейна, яка не була витрачена, тобто використовується в якості вхідних даних у новій транзакції [4].

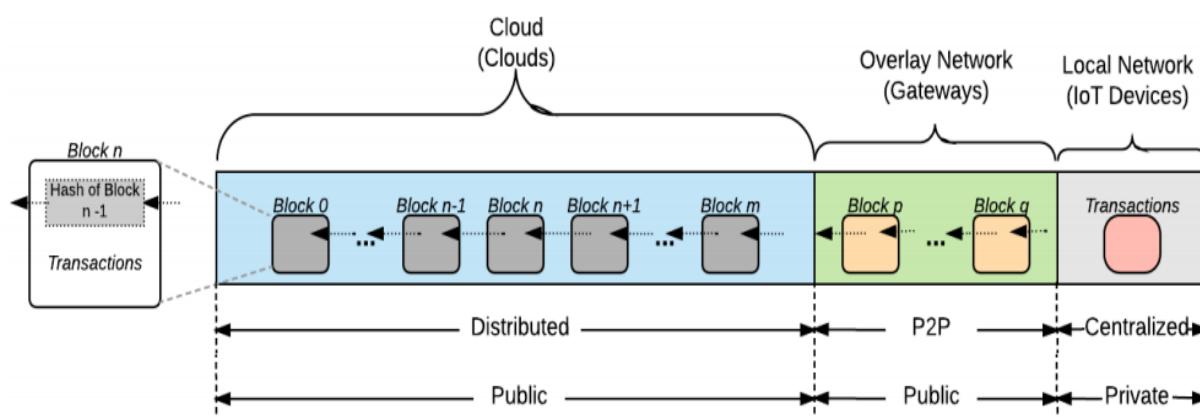


Рис. 2. Огляд запропонованої структури блокчейна.

Висновок. Технології blockchain та застосування цих технологій в системах IoT здобули велику увагу як у наукових колах, так і в галузі. Однак зберігати та керувати блокчейном в IoT-мережах є складною проблемою, завдяки масивним даним, що генеруються через програми IoT та обмеженим ресурсам в інфраструктурах IoT[5].

Література

1. L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," IEEE Transactions on industrial informatics, vol. 10, no. 4, pp. 2233–2243, 2014.
2. P. Johansson and E. Perjons, "Design principles for process modelling in enterprise application integration," information systems, vol. 26, no. 3, pp. 165–184, 2001.
3. M. Bartoletti, A. Bracciali, S. Lande, and L. Pompianu, "A general framework for bitcoin analytics," arXiv preprint arXiv:1707.01021, 2017.
4. D. Vorick and L. Champine, "Sia: Simple decentralized storage," Retrieved May, vol. 8, p. 2018, 2014.
5. K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," IEEE Access, vol. 4, pp. 2292–2303, 2016.

ПОЄДНАННЯ ТЕХНОЛОГІЙ БЛОКЧЕЙН ТА ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПОКРАЩЕННЯ ПРОЗОРОСТІ ТА ПРИВАТНОСТІ ДАНИХ

Поддубна М.О.

*Інститут телекомунікаційних систем КПП ім. Ігоря Сікорського, Україна
E-mail: maripod1210@gmail.com*

Combination of blockchain and artificial intelligence technology for improvement data clarity and privacy

Blockchain - a chain of custody of registrations, yakimit to corrode beyond the years of usa by the corridors to the extent. As a rule, there is a real basis for a new server-free internet technology, which is the basis for a new serverless internet technology. And particular intellect - as if it were a la carte, like a software program or a machine and the manifestations of "intellectual" health.

Блокчейн – це відкритий розподілений реєстр, яким користуються усі користувачі в мережі. Транзакції зберігаються в блоках разом з хеш значеннями і відмітками часу, кожен пов'язаний з попереднім і в результаті чого формується ланцюжок. Головною особливістю блокчейну є незмінюваність.

Штучний інтелект – це один з найперспективніших напрямків комп'ютерних наук, який вивчає методи розв'язання задач, для яких не існує способів вирішення. Системи штучного інтелекту мають можливості, що схожі на інтелект людини плануванням, навчанням, рішенням логічних задач, а також соціальними навичками та творчістю. З'являються розробки на зразок машин без водіїв, роботів-кур'єрів, проте разом з тим зростає занепокоєння. Зворотна сторона штучного інтелекту - від можливості фальсифікації новин з цілком реалістичними знімками, звуко- і відеозаписами до порушень права на особисту таємницю.

Блокчейн має чимало слабких місць, в тому числі з точки зору безпеки, масштабованості і ефективності, а штучний інтелект, в свою чергу, страждає від проблем, пов'язаних з можливістю порушення приватності, а також з відсутністю довіри і можливості пояснити принцип дії. Об'єднання цих двох технологій, схоже, неминуче - вони могли б взаємно доповнити один одного для створення принципово нового покоління цифрових систем.

Блокчейн може використовуватись як основа децентралізованих платформ координації для різних компонентів штучного інтелекту, включаючи дані, алгоритми та обчислювальні потужності. З використанням блокчейну штучний інтелект зміг би вийти на новий рівень масштабів та інновацій, а також всі рішення штучного інтелекту стануть прозорішими, зрозумілими і будуть заслуговувати довіри.

Штучний інтелект розвивається завдяки величезним обсягам даних, що потенційно доступні для дослідників, розробників, комерсантів. Дані – це цінність цифрової економіки, але доступу до них немає через бар'єри недовіри.

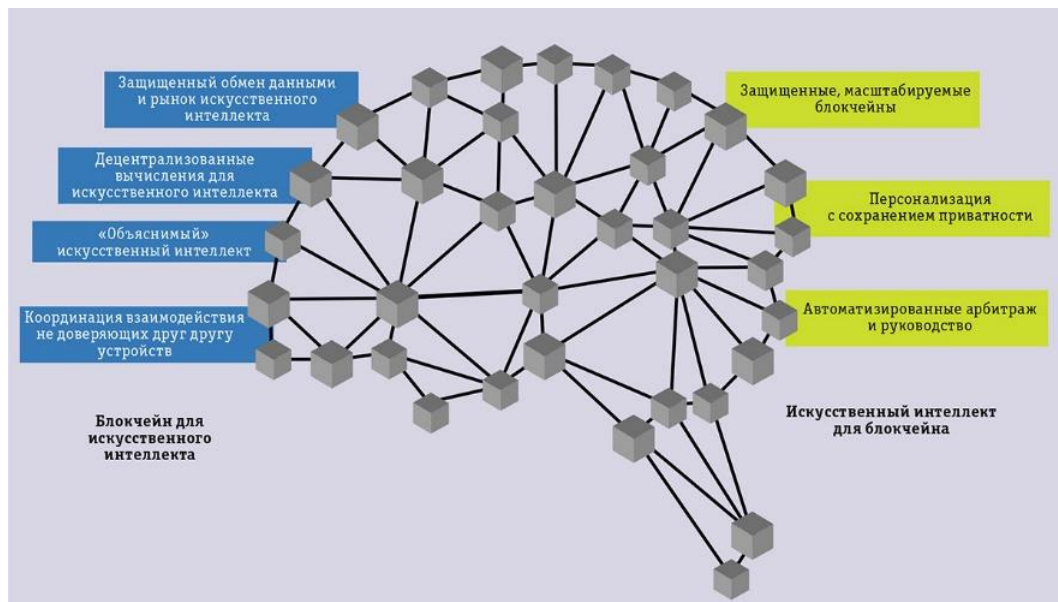


Рис. 1. Пример зв'язку між блокчейном та штучним інтелектом.

Блокчейн забезпечує прозорість і дозволяє з'ясовувати, до яких даних відбувався доступ і хто до них звертався. Користувачі зможуть ділитись даними з впевненістю, що дані будуть без порушень задіяні для персоналізації чи інших корисних застосувань. Розробка та експлуатація блокчейну вимагає настройки тисячі параметрів та компромісів між безпекою, продуктивністю та децентралізованістю і т.д. Штучний інтелект зможе полегшити прийняття цих рішень за допомогою автоматизації та оптимізації роботи блокчейну для більшої продуктивності та покращеного контролю. Враховуючи те, що блокчейн має загально доступні дані, то штучний інтелект буде грати ключову роль в забезпеченні конфіденційності та приватності користувачів.

З огляду на стрімкий прогрес машинного навчання, блокчейн, що працює під управлінням інтелектуального алгоритму, цілком міг би виявити факт атаки і автоматично включити захисні механізми. А якщо збиток неминучий, штучний інтелект міг би щонайменше ізолювати атакується компонент від решти блокчейн-платформи. Керуючи блокчейном, він міг би покращувати масштабованість і підвищувати надійність розподіленого реєстру. Тому поєднання цих технологій в найближчі часи є рішенням проблем як для штучного інтелекту, так і для блокчейну.

Література

1. Федотова Вероника Вячеславовна, Емельянов Богдан Георгиевич, Типнер Людмила Михайловна Понятие блокчейн и возможности его использования // European science. 2018. №1 (33).
2. Кирилова Дарья Александровна, Маслов Никита Сергеевич, Рейн Андрей Давыдович Blockchain, как новая технология для разработки // International Journal of Open Information Technologies. 2019. №1.
3. A REVIEW ON THE USE OF BLOCKCHAIN FOR THE INTERNET OF THINGS // FERNÁNDEZ-CARAMÉS T.M., FRAGA-LAMAS P. // presented at the IEEE ACCESS

ПРО ДОЦІЛЬНІСТЬ РОЗШИРЕННЯ ПОНЯТТЯ ІНФОРМАТИЗАЦІЇ

Гребенніков В.О.
E-mail: hreben@ukr.net

About expediency of expanding the informatization concept

The concept of informatization are most often associated with the rise in the use of the latest ICTs in recent decades. However, some researchers, including Schiller, Habermas, Giddens, Webster, believe that the essence of informatization should be linked to the expansion of the use of information in society, regardless of the technologies used, and that the informatization of mankind has been going on for several hundred years. The systematic extension of this logic allows to expand the concept of informatization to all information processes in the living nature, and not only to the process of anthropogenesis and development of human societies. This expansion of the concept of informatization allows us to get a new holistic view of the key role of information and processes of informatization in the processes of origin and evolution of life on Earth.

Поняття інформатизації набуло популярності в наукових, соціологічних і політичних дискурсах у другій половині 20-го і на початку 21-го століть, однак до сьогодні це поняття не має чіткого визначення. Найчастіше це поняття позначають такими термінами, як «постіндустріалізм», «інформаційне суспільство», «суспільство знань», «інформатизація», «цифровізація», «диджиталізація» тощо. Нечіткість термінології цього поняття веде до нечіткості постановки цілей і задач інформатизації суспільства, до неотримання очікуваних результатів інформатизації та до помилок у тлумаченні таких результатів. Помилки у спрямовуванні і оцінках процесу інформатизації мають негативні наслідки для суспільства, оскільки багато країн пов'язують з інформатизацією свої надії на економічний, соціальний і культурний розвиток.

Нечіткість поняття інформатизації стає явною, наприклад, при порівнянні визначень терміну «інформатизація» в україномовній та англійській версіях Вікіпедії.

В україномовній Вікіпедії наведено тільки одне, досить звужене визначення інформатизації із Закону України «Про Концепцію Національної програми інформатизації» – це «сукупність організаційних, правових, політичних, соціально-економічних, наукових, виробничих процесів, що спрямовані на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі застосування сучасної комп'ютерної і мережевої техніки».

В англійській Вікіпедії поняття інформатизації трактується більш широко і наведено чотири варіанти визначень терміну «інформатизація», два з яких варто процитувати:

1) це «ступінь, до якої географічний ареал, економіка або суспільство стає інформаційно орієнтованим»;

2) це «процес змін, що має особливості:

а) використання інформатизації та інформаційних технологій настільки є широким, що вони стають домінуючими силами в управлінні економічним, соціальним і культурним розвитком;

б) безпрецедентне зростання швидкості, кількісних характеристик і популярності у виробництві і розподілі інформації»

Між тим, після ознайомлення з узагальнювальними роботами за тематикою інформатизації, наприклад, [1-4], очевидно стає можливість більш простого, точного та, водночас, більш широкого визначення поняття інформатизації приблизно у такому формулюванні:

«Інформатизація – це поширення використання різноманітної інформації та інформаційних процесів для оптимізації життєдіяльності суспільства і кожного із його індивідів».

Френк Уебстер, досліджуючи в роботі [1] роль інформації в сучасному суспільстві, після аналізу робіт Шиллера, Хабермаса і Гідденса зауважує, що, згідно з переконанням цих авторів, більшу увагу слід приділяти інформатизації нашого способу життя і що цей процес інформатизації триває, можливо, вже кілька століть, хоча за останні десятиліття він прискорився. Завершує своє дослідження Уебстер твердженням про те, що зрозуміти причини сучасної вибухоподібної інформатизації можна лише з'ясувавши «якого типу інформація з'явилася, навіщо вона була потрібна, які групи у суспільстві її використали і для яких цілей».

Такі обґрунтовані думки Уебстера, очевидно, слід враховувати при уточненні поняття інформатизації і ні в якому разі не використовувати при цьому ознаки тих чи інших інформаційних технологій, які використовувались людьми протягом вже кількох століть. Тим більше, що науковці вперше почали відмічати явища «інформаційного вибуху» не в 60-70-ті роки 20-го століття під час швидкого прогресу радіомовлення, телебачення і комп'ютерних засобів, а в середині 18-го століття під час бурхливого розвитку поліграфічної промисловості і масового розповсюдження книжкової і газетно-журнальної друкованої продукції.

Логіка Уебстера щодо сутності процесу інформатизації людського суспільства, за якої увага фокусується саме на інформації, що циркулює в суспільстві, а не на сучасних електронно-комп'ютерних технологіях, що спричинили інформаційний вибух останніх десятиліть, є надзвичайно продуктивною. Дійсно, які б інформаційно-комунікаційні технології не використовувалися людством протягом його багато тисячолітньої історії, процес інформатизації людських суспільств не зупинявся і тільки набирив обертів. Хіба не були визначними етапами інформатизації людських суспільств винайдення писемності, формування і широке використання членороздільної (фонетичної) мови, формування родового устрою суспільства з найбільш мудрішим його очільником, який накопичував і використовував на благо суспільства інформацію від усіх членів роду? Очевидно, все це були етапи довгого інформаційного розвитку (інформатизації) людства, останніми з яких були етапи книгодрукування, газетно-журнальних ЗМІ, радіомовлення, телебачення, комп'ютеризації та Інтернету.

Логіка фокусування на інформаційних процесах, а не на інформаційних технологіях, веде до необхідності включення у поняття інформатизації також і біологічні інформаційні процеси, які покладені природою в основу буття і еволюції не тільки людини, як окремого виду тварин, а й усього тваринного світу.

Результати досліджень еволюційних біологів свідчать про провідну роль інформаційних процесів у еволюції усіх видів тваринного світу. Чим вища здатність того чи іншого організму до сприймання, оброблення і використання інформації з свого оточення та від своїх органів, тим вищу сходинку займає організм у класифікації тварин, тим стійкішим є конкретний вид організму в процесах біологічної еволюції.

За інформаційні процеси в організмі тварин відповідає нервова система з її центральним відділом – головним мозком. Еволюційними біологами давно вже підмічена закономірність збільшення розмірів і складності структури нервових систем і головного мозку по мірі розвитку видів тварин. Цю закономірність еволюції тваринного світу біологи означають спеціальним терміном «енцефалізація». В термінах інформаційно-комунікаційних технологій цю закономірність можна вважати просто довготривалим процесом інформатизації тваринного світу. Початком цього процесу слід вважати час появи перших нервових систем у найпростіших тваринних організмів, тобто приблизно 600 мільйонів років тому.

Таким чином, фокусування уваги на інформаційних процесах, а не на інформаційних технологіях, дозволяє розширити поняття інформатизації на увесь тваринний світ, одним з представників якого є людина розумна, а також розширити часові рамки процесів інформатизації тваринного світу приблизно до 600 мільйонів років – періоду, коли в тваринному світі виникли і вдосконалювалися нервові системи. Очевидно, що наявність нервової системи в організмі, її складність і здатність організму інформаційно реагувати на зміни оточення, є головним здобутком тваринного світу в процесі його довготривалої еволюції.

Нарешті, якщо узяти іще до уваги генетичні інформаційні процеси в усій живій природі, то поняття інформатизації має включати також і процес розвитку геномів різних організмів, включно з геномами найпростіших тваринних організмів типу вірусів, а також геномів усіх рослин, включно з одноклітинними водоростями. При цьому, часові рамки процесів інформатизації в живій природі можуть бути розширені на період приблизно 4 мільярдів років.

Задовольнити усім вищенаведеним особливостям процесу інформатизації у його визначенні можна прийняттям такого формулювання:

«Інформатизація – це процес все ширшого використання організмом або їх спільнотами зовнішньої і внутрішньої інформації задля оптимізації процесів своєї життєдіяльності та розвитку»

Таке визначення є достатньо широким і охоплює усі інформаційні процеси живої природи, включно з інформаційними процесами людини та людських суспільств. Однак воно має деяку невизначеність внаслідок нечіткості терміну «інформація», який досі не має загальноприйнятого визначення. Усунути цей недолік можна прийняттям такого додаткового визначення терміну «інформація» для сфери живої природи:

«Інформація – це малоенергетичний відбиток різноманітних природних і уявних сутностей у формі, яка є зручною для сприйняття, оброблення, маніпулювання, запам'ятовування і використання живим організмом або їх сукупністю у своїй життєдіяльності».

З урахуванням такого уточнення терміну «інформація», запропоноване розширене визначення поняття інформатизації набуває необхідної чіткості і може

бути використане для усього спектру процесів інформатизації, які слугують базою еволюції видів в живій природі, зокрема процесів інформатизації:

- людських суспільств;
- окремої людини (її соціалізації);
- усього тваринного світу (енцефалізації тварин);
- усієї живої природи на рівні генетичної інформації.

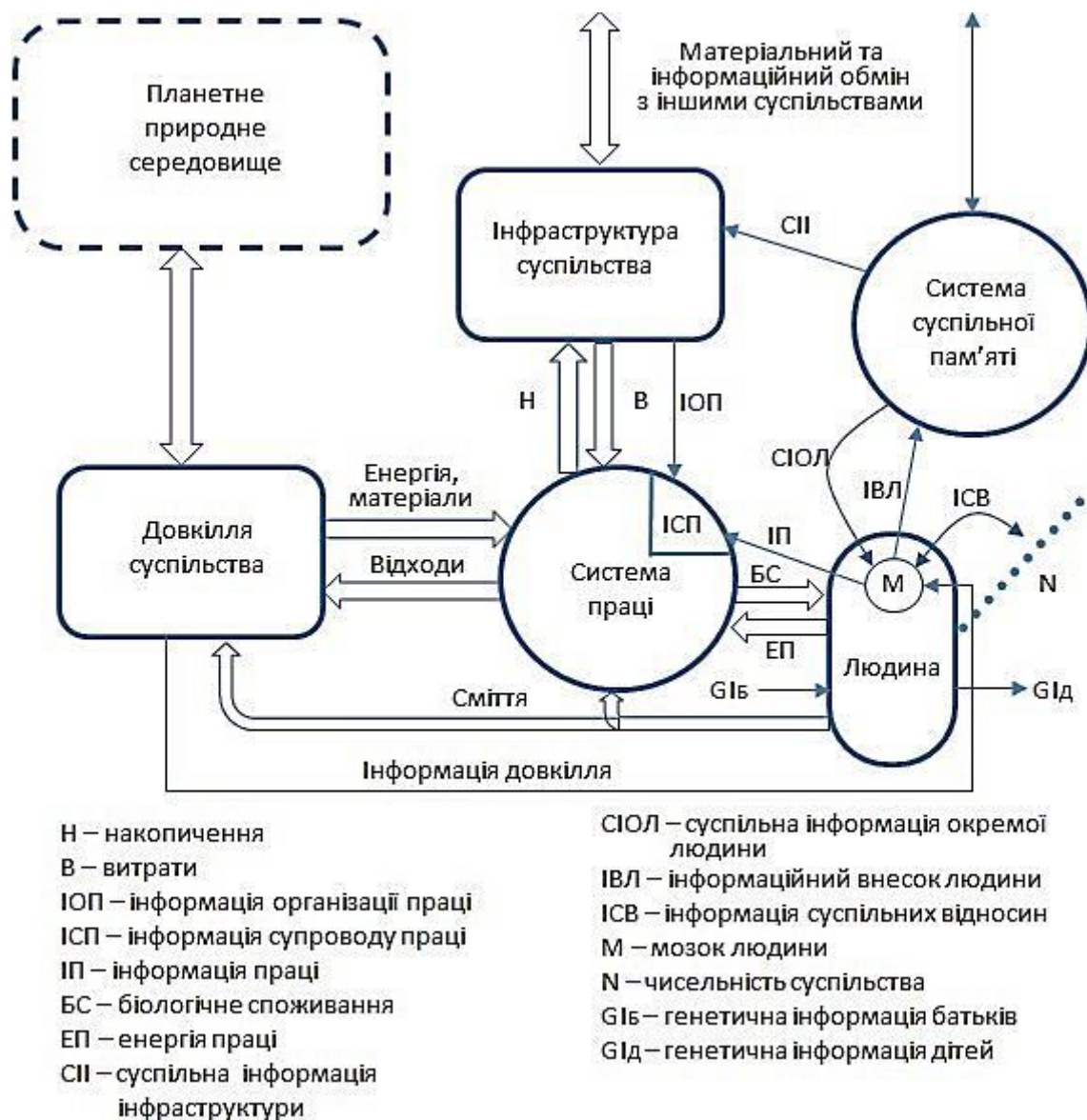


Рис. 1. Загальна схема інформаційного впливу на основні процесу життєдіяльності суспільства

Розширення поняття інформатизації посилює цілісний системний підхід у дослідження еволюції усіх форма життя на Землі, у тому числі, й окремого виду тварин «людина розумна» та людських спільнот (суспільств). За такого розширення, інформація стає таким же повноправним чинником існування і розвитку живої природи, як матерія та енергія. Зайвий раз підтверджується геніальне у своїй простоті визначення інформації, яке дав Норберт Вінер: «Інформація є інформація, а не матерія і не енергія». Тепер з повним правом можна стверджувати, що без інформації і активних інформаційних процесів не можливі ні

зародження, ні еволюція, ні майбутнє живої природи. Для людини і людських суспільств, як найбільш інформаційно-розвинених форм життя, інформація і процеси інформатизації стають ключовими і визначають не тільки технологію, економіку і соціальні відносини, а й їх близьке і далеке майбутнє. Такий висновок, мабуть вперше, був зроблений на початку 20-го століття Шарденом і Вернадським при обґрунтуванні ними вчення про ноосферу.

Сьогодні інформаційні процеси в житті людських суспільств явно недооцінені – основна увага приділяється економічним, енергетичним і політичними процесам. В той же час, неважко помітити, що рівень розвитку суспільств визначається тією інформацією, яка накопичувалася в цьому суспільстві протягом його історії. Так само і рівень розвитку особистості в суспільстві визначається тією інформацією, яку ця особистість сприйняла і накопичила в процесі своєї соціалізації. Варто зауважити, що новонароджена людина, отримавши повний масив (46 хромосом, 12 Гбайт) генетичної інформації від своїх батьків і предків, має пусту робочу і довготривалу пам'ять, в якій лише поступово накопичується інформація, необхідна для повноцінного життя особистості в людському суспільстві. Цей процес соціалізації новонародженої людини є ніщо інше як процес індивідуальної інформатизації.

Висновки. Розширення поняття інформатизації на усю сукупність процесів сприймання, оброблення, маніпулювання, зберігання і використання інформації в живій природі, одним з представників якої є «людина розумна», доцільно з системної (узагальнювальної, холістичної) точки зору і відкриває нові можливості поглибленого дослідження усіх форм життя живої природи, зокрема:

- пояснення феномену стрімкого розвитку людських суспільств протягом останніх кількох тисяч, а особливо останніх 300 років, при незмінності біологічних властивостей людини та її природного оточення;
- обґрунтування критичності кількості і якості інформації, яка циркулює в суспільстві, для процесів інформатизації (соціалізації) індивідів у цьому суспільстві, а також для визначення структури, напряму і темпів розвитку суспільства;
- ліквідація прогалини між природними інформаційними процесами та штучно створюваними людьми інформаційними процесами для об'єктивного визначення їх взаємних впливів та об'єктивної оцінки користі або шкоди штучних інформаційних процесів;
- логічне пояснення феномену енцефалізації тваринного світу як прояву універсального принципу економії матеріальних і енергетичних витрат організму за рахунок більш інтенсивних, більш складних але малоенергетичних інформаційних процесів.

Література

1. Френк Уебстер. Теории информационного общества // Изд. «Аспект пресс», М, 2004.
2. Christian Fuchs. Internet and Society: Social Theory in the Information Age / New York: Routledge, 2008.
3. Валерий Гребенников. История и перспективы информационного общества// LAP Lambert Academic Publishing/Saarbrücken, 2014.
4. Гребенников В.О. Суспільство, економіка, інфокомунікації та сталий розвиток України // Економіка розвитку, № 4/2015, № 1/2016.

SEMINAR
Modern information and telecommunication trends

УДК 004.9

INTERNET OF THINGS AND 5G

Mikhnenko Yaroslav

*Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: yaroslavmikhnenko@gmail.com*

Інтернет речей та 5G

Сьогодні світ знаходиться напередодні нової технологічної революції в бездротових мережах. Очікуваний запуск п'ятого покоління стільникового зв'язку тісно пов'язаний з розвитком не менше проривного явища останніх років - Інтернету речей (IoT). Обидві ці концепції здатні кардинально змінити бізнес і соціум, надавши їм унікальні можливості взаємодії «розумних» пристроїв.

Today, the world is on the eve of a new technological revolution in wireless networks. The expected launch of the fifth generation of cellular communications is closely linked to the development of at least a breakthrough in recent years - the Internet of Things (IoT). Both of these concepts are capable of dramatically changing business and society, giving them unique opportunities to interact with "smart" devices.

It is already becoming apparent that the IoT concept is capable of making revolutionary changes in business, society and the management system of virtually any technological process. The Internet of things, sooner or later, will unite all those involved in the manufacture and use of "smart" equipment into one global system. However, one of obstacles to do this is the lack of network capacity, which does not allow you to use all the features of IoT.

The use of the next generation of mobile communication - 5G, can play a major role in addressing this issue. Its main difference from the previous ones is the huge (over 10 Gb / s) data transfer rate, and, accordingly, the response speed. The signal delay in 5G will be reduced to only 1 ms, despite the fact that in 4G it is 10 ms, and in 3G – all 100 ms.

But in the context of using 5G IoT devices, speed is still not a determining factor. The minimum signal delay, reliability of the network and the ability to massively connect various "smart" devices with their specific tasks and the uninterrupted interaction between them come to the forefront.

Although it seems that the world has come close to implementing 5G, developers still have a lot of work to do. The global compilation and development of the IMT-2020 communication standard (officially named 5G technology) is entrusted to the International Telecommunication Union. At the country level, implementation will fall on the shoulders of both telecom operators and providers and the government. It will require the restructuring of the existing infrastructure for a new generation of communications.

At the same time, 5G will not immediately replace 3G and LTE, but will

work in parallel so that gadgets can be able to switch between networks depending on user's requests. Given the current level of technological equipment of mobile operators, at the first stage, the signal coverage of 5G networks will be even less than that of 3G and LTE. Most likely, at first the base stations will be located along the main routes, business centers of large cities, and as the new infrastructure develops, they will go to the "outback".

Customizing to new standards will have not only infrastructure, but gadgets and all other devices connected to the network. To fully work in 5G, they must become not only "smarter", but also more powerful. Another major challenge that 5G developers will have to solve is to reduce power consumption. This parameter is especially relevant for all kinds of sensors and other IoT devices. To solve it, in all likelihood, higher frequency ranges and the connection of mobile networks with WiFi technology will be used.

In any case, the new generation of 5G communications will become the basis for the digital transformation of business and society, and the effect of its implementation will go far beyond the IT sphere.

How will 5G and IoT change the world? Today, high-tech provides many additional features for various gadgets with access to the Internet. This function is unifying for IoT devices. Since the capabilities of the 5G network are truly huge, its appearance will definitely lead to a sharp increase in the number of "smart devices" and the evolution of existing ones. Simply put, the potential of the new communication standard will facilitate the connection to the network of everything that can be connected, from household appliances to aircraft. According to some estimates, the number of simultaneous connections can reach from 50 to 100 billion devices.

But the main difference between 5G and previous generations will be that it will carry out a new revolution in business processes. The entertainment sector will continue to occupy a large place in the life of society, but nevertheless, it will have to give way to advanced technologies, such as IoT and VR. Modern business has long lived in the "digital" category and just waited for the next round of productivity, so the high speed, short response time and low power consumption that 5G promises will ensure the mass implementation of robots and the Internet of things.

This, in turn, will "turn" many traditional areas of wireless networks, introducing hundreds of millions of online objects that perform a variety of functions. Actually, 5G will become a kind of framework around which the image of a new, digital economy will begin to form, actively using IoT technology, multiplying the already known advantages of the latter and bringing it closer to widespread use.

Currently, it is still not possible to fully integrate wireless devices into a single network. The main obstacle is the lack of a single standard for IoT, since different network protocols are now used in its different segments. But 5G technology, designed to work with heterogeneous traffic, can provide a variety of devices with different parameters, both familiar mobile and smart ones, such as sensors, regulators and other devices that can be connected to the Internet.

The social component of IoT .If the technical side of launching a new network is more or less clear, then the problem of restructuring thinking for the mass development of IoT will only have to be solved. Of course, the introduction of 5G will lead to a breakdown of existing standards in everyday life and business. And if the latter will have to adapt in one way or another in order to survive, the ordinary users are not yet ready for such changes. And, first of all, this concerns the availability of information about the capabilities of IoT systems and their proper use.

What is the use if disparate devices are closed on one or two systems or groups of people and perform a limited range of tasks? And if it is technically possible to solve this problem by integrating various platforms and services, for users, individual companies have already begun developing a special concept called the Social Internet of Things (Social IoT or SIoT).

In short, its essence is to create a service platform that combines people and devices into one global social network. The unlimited possibilities of such a network to receive and accumulate colossal streams of information connected to devices capable of independently generating content will allow you to design various services with almost any configuration, while obtaining the right products or solutions.

At first glance, all this may seem like something that goes beyond the ordinary user's understanding, but the whole point of Social IoT lies precisely in the mass availability of information about the capabilities of “smart” devices and the simplicity of its exchange.

In other words, the main task of Social IoT is to create a single information space that is accessible and understandable to any person.

Of course, a detailed description of Social IoT's ability to combine real-world devices with the virtual world requires separate material. Nevertheless, from what has already been said, it becomes clear that the number of tasks that can be solved through Social IoT after the launch of 5G is simply unlimited. And someone who wants to keep up to date and feel confident in the digital world of “smart” devices surrounding him should prepare now, because then you will have to spend time and money on training.

References

1. Unet. Интернет вещей и 5G: Концепція майбутнього [Електронний ресурс] / Unet. – 2019. – Режим доступу до ресурсу: <https://habr.com/ru/company/unet/blog/336936/>.
2. 5G в Україні [Електронний ресурс] // УКРІНФОРМ. – 2020. – Режим доступу до ресурсу: <https://www.ukrinform.ua/rubric-technology/2820416-v-ukraini-5g-zavitsa-ne-ranise-niz-cerez-tri-roki.html>.
3. Макаренко Ю.В. Аналіз можливостей використання технологій 5G в системах Інтернету речей / Макаренко Ю.В.. // ElectronAcoustEng. – 2019. – С. 45–51.
4. Social Internet of Things (SIoT): Transforming smart object to social object [Електронний ресурс] / Deboleena Dutta, Chido Tazivazvino, Surajit Das, B.K. Tripathy. – 2017. – Режим доступу до ресурсу: https://www.researchgate.net/publication/287216756_Social_Internet_of_Things_SIoT_Transforming_smart_object_to_social_object.

“SMART STREET” MANAGEMENT SYSTEM PROTOTYPE BASED ON THE LORAWAN PROTOCOL

Kopaniev M¹., Zhivkov O²., Rybak O².

¹Physico-Technical Institute Igor Sikorsky Kyiv Polytechnic Institute

²Institute of Telecommunication Systems Igor Sikorsky Kyiv Polytechnic Institute

E-mail: morbiyccc@gmail.com; zhivkovalex@gmail.com

Прототип системи управління “Smart Street” на основі протоколу LoRaWAN

Актуальною і важливою задачею місцевої влади є зменшення використання енергетичних і людських ресурсів у сфері обслуговування вулиць. Вирішення даної задачі потребує розробки прототипу системи управління, яка дозволить автоматизувати процес керування вуличним освітленням, моніторингом вільних місць для парковки і своєчасним вивозом сміття. Для кожного з виділених завдань було розроблено прийомопередавачі із власним набором сенсорів. У роботі запропоновано використання протоколу LoRaWAN для передачі даних від спроектованих сенсорів до центру обробки. За результатами розробки представлено прототип додатку для управління “Smart Street”.

Today an urgent and important task is to reduce the use of energy, time and human resources. Proper planning of sequence of certain system tasks execution is one of the possible solutions to this problem. However, at a certain point, the exclusively rational resources usage ceases to be effective. Automation based on the concept of the Internet of Things (IoT) can be a modern solution to the problem.

According to Cisco’s research, 500 billion devices connected to the Internet are expected by 2030 [1]. Each such device combines certain sensors that interact with the internal and external environment. As data generators, these devices have access to the global network. Connecting such devices into a single structure is called the Internet of Things. IoT devices not only become a source of information, but also automate processes that can affect the state of the environment.

A growing trend to solve the problem of excessive resources usage is the introduction of the Internet of Things technologies in an urban environment. Municipal authorities thus exercise cheaper control over various industries such as water supply, timely garbage collection, road traffic control and parking lots. And besides, effectively used weather data, lighting management, atmosphere quality control and early earthquake detection. In addition to the obvious financial and social benefits, officials receive an increase in the public confidence rating. A useful bonus of implementing the Internet of Things is the collection of all kinds of depersonalized helpful data, so that authorities, mobile operators and client-oriented companies better understand the audience by offering high-quality demanded services.

A possible scenario for the development of the “Kiev Smart City” concept is to design an automated elements management system prototype for the “Smart Street”. Introduction of the following controlled spheres are proposed:

- street lightning maintenance based on the illumination parameter;
- checking of parking spaces congestion degree;
- scheduling of garbage containers cleaning.

This choice is due to the following practical factors: in Barcelona smart lighting technology can save up to \$ 37 million a year, parking spaces booking applications allow

the city to earn 50 million euros a year. In addition, it simplifies the search for electric vehicles charging station, and it is easier for municipal authorities to control traffic congestion [2]. In Chicago, the sensors installed in garbage containers allowed reducing the number of garbage ignition by 32%.

For the “Smart Street” management system implementation the following steps are proposed:

- selection of data transfer protocol;
- creation of three necessary sensors types;
- setting up the base station and Network server;
- development of an Application server.

One of the popular urban-oriented data transfer protocols is LoRaWAN (Long Range Wide Area Network). It allows devices to exchange small information volumes (up to 254 bytes per message) at a very low (0.3-50 kbit/s) speed. Collecting information from scanners is safe for human health since the transmitter power reaches only 25mW [3]. The communication nodes hierarchy consists of an end device (sensor), a data exchange gateway, a Network server, and an Application server [4]. The trade-off between message transmission range and speed allows using the end device with an internal power source up to 10 years. The frequency standard for Europe (including Ukraine) is 868 MHz, which is not licensed under the laws of Ukraine, and the bandwidth is 125-500 kHz. The LoRaWAN protocol provides mandatory two-level encryption with the AES-128 standard (CMAC) to ensure message integrity. One base station coverage ranges up to 5 kilometers in an urban environment.

An important objective of this work is to develop transmitter capable to work on the LoRaWAN protocol basis. This decision is due to the cheaper production of future integrated systems, as well as the personal transmitter settings possibility. As a computing unit, the use of Arduino Nano microcontroller is proposed. Its main advantages are the availability of non-volatile memory (EEPROM) and support for SPI (Serial Peripheral Interface).

To work on the LoRaWAN protocol basis, a modem, receiver and signal transmitter are required. The modem is responsible for using the desired type of modulation, as well as encoding and decoding information. In addition, the modem provides synchronous and asynchronous operation modes. In view of modern integration trends, the modem, receiver and transmitter are made in the single chip form. For compatibility with Arduino Nano, the RFM95W chip manufactured by HopeRF was chosen. Its choice is due to the presence of the ready-to-use open library LMIC (LoRaWAN-in-C), which is compatible with Arduino Nano, as well as the lack of the need to use power regulators, as the microcontroller and chip have the same supply voltage.

The developed transmitter needs to be registered in the LoRaWAN network. Therefore, it is necessary to configure precisely two main system topology components: the gateway and the Network server. The gateway is configured by installing special software - Packet Forwarder (PF). Every Network server provides its own PF for downloading, so there is a need in choosing a reliable one. The popular and convenient Actility service was chosen as the Network server, the team of which took part in the LoRaWAN protocol creation. After installing the software, the base station has to be registered to Actility. The last configuration step is to register the created transmitter, after which it will be possible to observe incoming data packets in Actility Wireless Logger.

The last stage in the control system development is the selection of an Application server for decrypting messages and interpreting monitoring results. The most convenient option to satisfy all the system needs is to create processing program. It is proposed to use an application written in the LabVIEW development environment as a prototype (Fig. 1). As the main functionality, it is worth highlighting: the presence of a message decoder, the ability to save the readings history in a MySQL database or as a Word format report, alarm signals flexible configuration and a graphical information representation.



Figure 1. The NI LabVIEW developed application.

Conclusion: As a result of the development of the “Smart Street” management system prototype, the following goal was achieved: the transmitters creation as well as the gateway and the Network server configuration, which together made it possible to establish the network based on the LoRaWAN protocol. In addition, in the work an Application server prototype is presented, that allows automated monitoring and control of the created system parameters. Future work will be devoted to expanding the devices range, creating a physical street prototype as the the sensors implementation form, as well as improving the processing program.

References

1. Cisco.com. (2016). At-a-Glance. [online] Available at: <https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf> [Accessed 10 Feb. 2020].
2. Iotnewsportal.com. (2018). How Smart City Barcelona Brought the IoT to Life. [online] Available at: <https://www.iotnewsportal.com/cities/how-the-smart-city-barcelona-brought-iot-to-life>.
3. Kopaniev, M. (2019). SMART GARDEN CONTROL SYSTEM DEVELOPMENT BASED ON LORAWAN PROTOCOL. In: Science and Technology of the XXI Century. Kiev, pp.88-89. Available at: http://konfist.fl.kpi.ua/sites/default/files/part_i_sections_1-5.pdf.
4. M.M. Kopaniev, D.O. Progonov (2019). Bezdrotova systema zv'yazku davachiv perymetral'noyi systemy okhorony na osnovi protokolu LoRaWAN [Sensors wireless communication for perimeter security system based on LoRaWAN protocol]. Teoretychni i prykladni problemy fizyky, matematyky i informatyky - Theoretical and applied problems of physics, mathematics and computer science: Proceedings of the International Scientific and Practical Conference. (Vols 1), (pp 124-125), Kyiv.

SECURE IOT DEVICE AUTHENTICATION

Minochkin D., Sushyn I.

National Technical University of Ukraine

“Igor Sikorsky Kyiv Polytechnic Institute”

E-mail: dmytro.minochkin@gmail.com, rubin26898@ukr.net

БЕЗПЕЧНА АУТЕНТИФІКАЦІЯ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ

У статті наводиться опис способу аутентифікації пристроїв інтернету речей та користувацьких пристроїв за допомогою хмарної технології з використанням цифрових сертифікатів. Наведено структуру мережі на основі інфраструктури відкритого ключа.

The growth of number of intelligent devices will create a network rich with information that allows supply chains to assemble and communicate in new ways. The technology research company “Statista” predicts that there will be above 74 billion installed units on the Internet of Things (IoT) by 2025 [1].

The Internet of Things (IoT) provides the ubiquitous connection between devices with sensitive and communication capabilities. IoT programs include healthcare, smart cities, smart grid, automotive, industrial applications, etc. [2], [3], [4]. IoT provides a large-scale deployment of communication between the device and machine to machine. The low complexity and low energy requirements for these devices pose security problems [5].

IoT device authentication is a vital step in key validation and key sharing, otherwise systems are open to attacks such as man-in-the-middle. In various studies and literature reviews security issues have been discussed, however, due to the lack of emphasis on a more structured and robust security architecture, security and privacy issues still remain. Thus, IoT authentication, access control, and intrusion attacks are major security issues you may encounter when implementing an IoT system.

In the proposed platform we focused on these security issues and offered a secure platform that allows user and IoT device to log on to a cloud server using a digital certificate. Once the registration process is completed, only the actually registered user can access the IoT device available on the network.

The platform (shown in Figure 1) is based on the Public Key Infrastructure

(PKI) system that manages certificates, systems, and applications to uniquely identify users, services and devices used on the network. An effective PKI should be transparent and comply with security principles, especially authentication and data integrity. This platform consists of IoT devices, users, cloud, certification authority (CA) and registration center (RA). Before connecting, IoT users and devices must be registered in the cloud with their verified digital certificate.

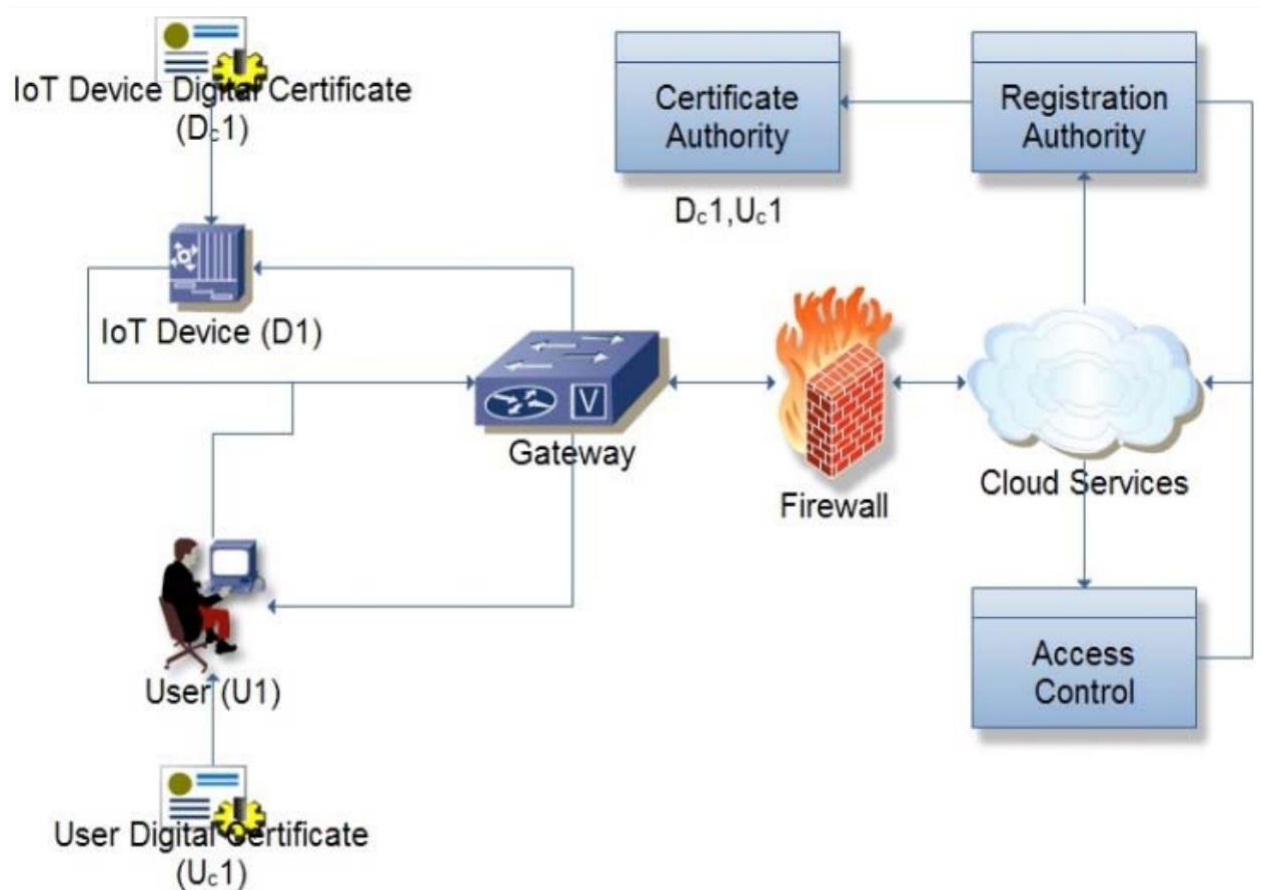


Fig. 1. Security platform for Cloud based IoT Network.

These certificates can be obtained from the RA. Here, the cloud application authenticates itself through PKI, but then issues certificates to the devices and users. Therefore, the cloud application also issues a separate certificate for the device, and for users these certificates are displayed as Dc1 and Uc1. The third and most important element in this platform is the centralized cloud, in which all devices, users and certificates with the corresponding keys Dc1, Uc1, ... are stored and indexed in their central repository. The registering authority provides the PKI binding, which is additionally linked to the CA certificate.

When a user registers, the cloud application checks the user's identity (for example, using the second factor, such as a voice call or SMS) before generating a

certificate for storage in the central cloud and issuing the certificate to the user application through a properly protected TLS channel. The device also has a unique certificate issued by the vendor. The device certificate and a unique device ID (included with the certificate) can be set before sending. When the user wants to use the device, the cloud app checks the user's certificate from the cloud index and access control defined in the management system.

Available Public key certificates require the following services: certificate storage; creation and revocation of certificates; key store management. The management system contains backup/restore keys; non-repudiation of digital signature systems; automatic update of key pairs and certificates. These digital certificates contain information such as the public key, name and expiration date of the certificate. The Certification authority is an integral part of PKI, as it is a source of trust and provides services to ensure an individual level of authentication of business units in the information exchange.

Conclusion. The proposed security structure based on PKI and implemented on IoT network is expected to be robust and very secure as it covers the major gap that exists in the application layer of the IoT infrastructure. In particular the work is focused on the systems authentication: device-to-cloud, user-to-cloud and user-to-device. It will also reduce the costs associated with the loss and allow new services to be introduced.

References

1. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 // - Access mode: <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>
2. L. Atzori, A. Iera, and G. Morabito, The Internet of Things: A survey.: Computer Networks, 2010, vol. 54, no. 15, pp. 2787–2805.
3. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash. Internet of Things: A survey on enabling technologies, protocols, and applications.: IEEE Commun. Surveys Tuts., Fourth Quarter 2015, vol. 17, no. 4, pp. 2347–2376.
4. S. Mumtaz, A. Bo, al-Dulaimi and K.Tsang. Guest Editorial 5G and Beyond Mobile Technologies and applications for Industrial IoT.: IEEE Transactions on Industrial Informatics, June 2108, vol 14, no. 6, pp. 2588-2591.
5. J. Zhang, Trung Q. Duong, R. Woods, A. Marshall. Securing Wireless Communications of the Internet of Things from the Physical Layer, An Overview: ResearchGate, 2017.

THE ARCHITECTURAL CONCEPT BONWIN "SMART ROOM"

Noskova D., Minochkin D.

National Technical University of Ukraine

"Igor Sikorsky Kyiv Polytechnic Institute"

E-mail: noskova.ds1007@gmail.com

Архітектурна концепція BONWIN "SMART ROOM"

У статті наводиться використання та структура архітектурної концепції Bonwin "Smart Room" для Розумних Будівель.

We are used to thinking that the smart home automation system is installed only in a home or apartment, but this is not the case. Now this system is installed in public places like hospitals, hotels, schools, etc.

I want to give you one example like Bonwin's "SMART ROOM". It is a smart hotel what not only designed to provide room for comfort but also to save energy and intended to prevent accidents.

When hotel is larger, then its management is bigger too. In recent years, the smart hotel room management system is popular. It has provided managers with comfortable and humanized controls. No matter how larger the hotel, it can still achieve effective management.

The main functions of this system are:

- providing comfort in the room;
- control and significant energy savings.

Main equipment

Through the rooms management host (RCU), let the main electrical equipment be centralized control and managed, and through the local area network and computer real-time communication the states.

By this method, management computer can control all of the equipment very convenient.

At the same time, electric equipment running status information will also be real-time sent to the management computer.

Hotel management service staff can omni-directional, all-weather master room state, control room equipment operation mode and parameters, and change the passive control into active control, let the experience management into science management.

The climate controller will allow to keep the room temperature always in a comfortable state, even when the visitor is absent.

The staff communication buttons will help you understand when to leave the room and not to be disturbed. You can easily forget about the inconvenient nameplates, now staff messages will be displayed in the panel of each room's e-number, and a signal will be sent to the host computer.

This system gives you the unique ability to remotely control the electricity in

each room.

A smart management system can manage all aspects of a hotel, which not only facilitates hotel management but also enhances hotel efficiency and service levels.

TCP/IP communications protocol

This system with international standard TCP/IP and Ethernet technology, can have operate on the hotel current network directly, also can be made as the separate special LAN.

Each RCU box have independent IP network address, which can comprehensive compatible with IEEE802.3 Ethernet standard.

TCP/IP communication protocol method: RCU equipment cost is not low, but it has many strong advantages in the system stability, reliability, advancement, data transmission capacity, convenient maintenance, low maintenance costs, etc.

So that the TCP/IP is the best communications protocol for the hotel guest control system.

Main Features:

- Guest can enter into his room without check in at the front desk.

Guest can use the booking, or Self-help registration machine to check in, not need go to the front desk. With Bonwin Networking lock system, the guest can use his member card to enter into the room, protect guest privacy, avoid the waiting at the front desk, help guest save time, help hotel to Attract more guests.

- Advanced stable TCP/IP communications protocol.
- Innovative, unique visual cat's eye, very convenient.
- Humanized design of 4 modes of lighting.

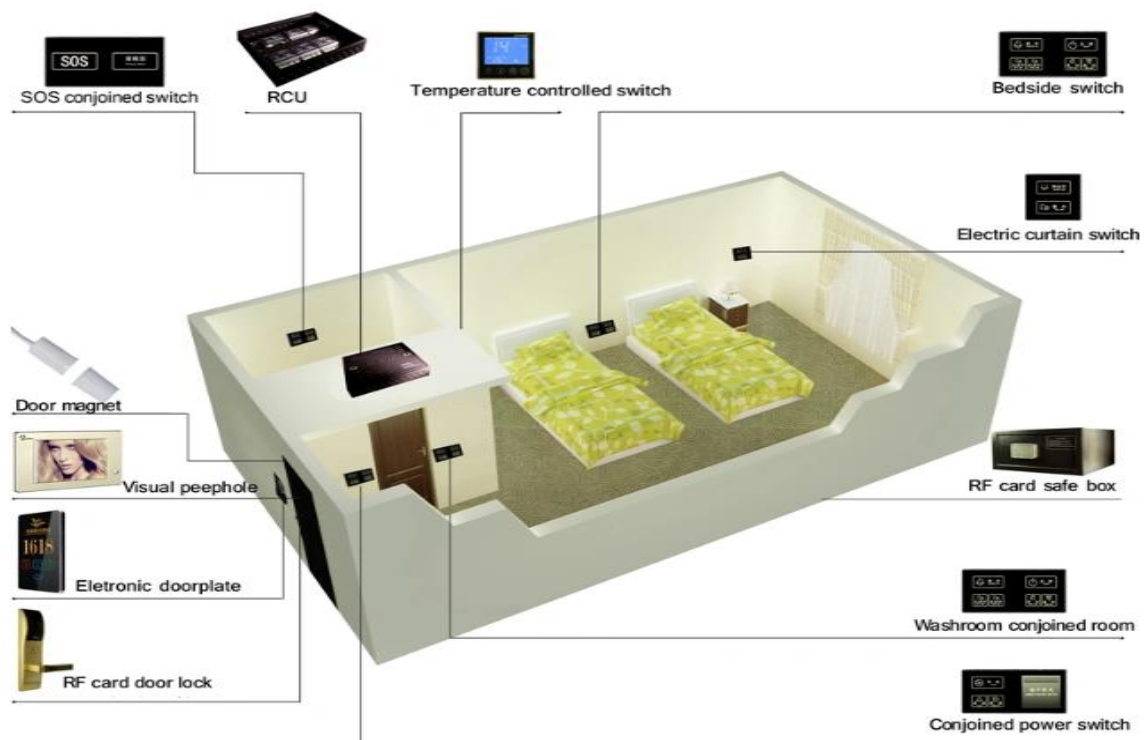


Fig. 1. Hotel room management system.

Light mode like visitor, reading, TV and sleep, let a guest feel more convenient and thoughtful.

- More convenient for guest, more efficient management for the hotels

Using one set software and the same database to unified management, hotel bring great convenience for the guest and hotel.

The system consists of:

- Management host (RCU) - makes it possible to remotely control and monitor all electrical appliances in the facility.

- Air condition temperature controller - monitors and controls room temperature.

- Personnel communication panel - allows you to call staff, include a sign "Do Not Disturb", "It's time to clean" and more.

- Energy saving switch - connects to the control unit. Allows you to turn off / on all the electricity in the room. Works from a room card or from any hotel card

- Visible cat's eye - is automatically activated when a doorbell rings or when a button is pressed on the display.

- Smart switches - special switches with engraving on keys: bed switches, for a bathroom, corridors and others. Connects to the control unit.

- Electronic room - allows you to specify a room number as well as other additional information.

- Doorbell rings.

- Electronic safe - connects to the control unit and opens with a key card from the number.

- Management software.

Saying all above, we can confidently say that IoT can be used not only private places but also in public. Such as hotel, hospital, school and etc. It will help to staff in work, to provide comfort, save energy, water and intended to prevent accidents. IoT opens up many possibilities for us, and it is necessary to wisely use it.

References

1. УМНЫЙ ДОМ для гостиниц <http://e-locks.ru/katalog/gostinichnye-zamki/sistema-upravleniya-komnatoj>
2. How Is The Smart Room Control System Linked To The Hotel?
<http://www.bonwinlocks.com/Article/howisthesmartroomcontrolsystem.html>
3. How Does the Bonwin Hotel Room Control System “Save Money“ for the Hotel?
<http://www.bonwinlocks.com/Article/howdoesthebonwin.html>
4. Smart Hotel Guest Room Control System <https://bonwintech.en.made-in-china.com/product/FSdJqrZjQBkx/China-Smart-Hotel-Guest-Room-Control-System.html>.

**RESEARCH AND IMPLEMENTATION
OF IOT TEMPERATURE AUTOMATED METERING PROJECT
BASED ON TELECOMMUNICATION SYSTEMS INSTITUTE**

Yatsyshyn O., Maltsev A., Dykyy A., Osypchuk S.

*Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: serg.osypchuk@gmail.com*

**Дослідження та реалізація IoT проекту для автоматизованого
вимірювання температури на базі інституту телекомунікаційних систем**

В роботі представлено результат дослідження та практичної реалізації проекту Інтернету речей для автоматизованого збору телеметрії, а саме – температури, що реалізований на кафедрі телекомунікаційних систем інституту телекомунікаційних систем, з можливістю доступу до зібраних даних з будь-якої точки Землі в мережі Інтернет та можливістю кастомізації їх представлення.

The paper presents a research and practical implementation result of the Internet of Things (IoT) [1,2] project for temperature values automated collection. The project is implemented at Telecommunication Systems department of Telecommunication Systems Institute. It aims the possibility to access the collected data from anywhere on the Internet and to customize data representation.

One of good **definitions** for **Internet of Things** is the following. IoT is a network of physical devices equipped with sensors, electronics, software, communication technologies, *with purpose to interact* with one another or with external environment, that is *designed and built* for purpose of restructuring economic and social processes, and eliminating the need of human participation which leads to *increased efficiency and reduced human workloads*.

The officially approved **students' circle of interests** "Researchers of wireless technologies for information transmission in the Internet of Things systems" operates in the Telecommunication Systems Department of Telecommunication Systems Institute since it was established in 2018. This students' circle covers both **research** of building IoT systems theoretical aspects and relevant information transfer technologies, as well as **practical implementation** of IoT projects.

The **problem solved** in this work is *the need to involve significant human resources to measure and record information on a regular basis about temperature in the lecture rooms of Telecommunication Systems Institute educational building* for the purpose of further data analysis and temperature control.

The **task solved** for mentioned problem above is the *IoT solution implementation for automated temperature data collection in the educational building* for the purpose of its further analysis and temperature control.

Since the automated temperature data collection had to be implemented in the educational building with **220V power supply** and with the ability to connect

via WiFi **IEEE 802.11** access points to Internet, the decision was made to use these available resources to build a cost-effective solution, i.e. less expensive and without involving to the solution any additional power sources and without any additional information transfer technologies.

The data from these temperature sensors are transmitted to the **MySQL database** hosted on the Internet. The scheme of the implemented solution with two temperature sensors is shown on Fig. 1.

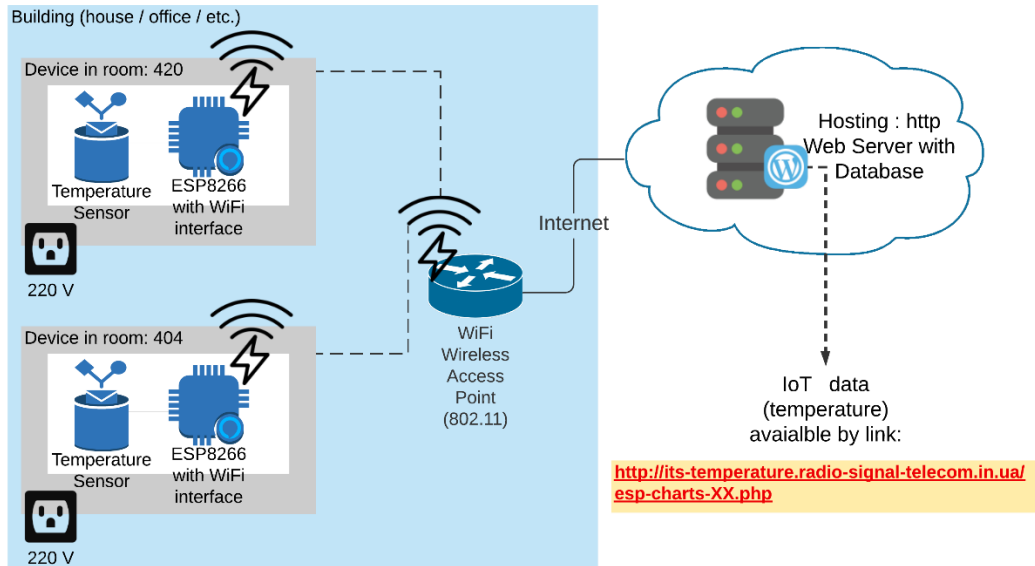


Fig. 1. Scheme of IoT project for automated temperature data collection.

The hardware of the solution is based on temperature sensors **DHT11**, **DHT21**, **DHT22**. These sensors connect to the NodeMCU V3 **ESP8266** (CP2102) transceivers. The ESP8266 have integrated wireless WiFi module (**IEEE 802.11**). The DHT temperature sensor with the ESP8266 board are mounted to a **plastic box** with intentionally made **holes** for ventilation and precise temperature measurement.

The sensors, transceivers boards, designed and developed **device** for measuring and transmitting temperature values are shown on Fig. 2.

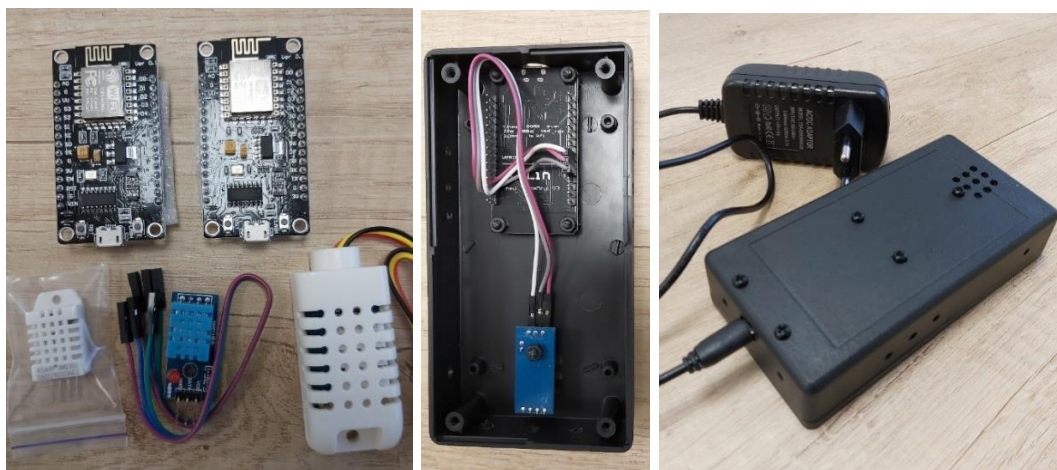


Fig. 2. Sensors, transceivers, built device for measuring and transmitting temperature.

The **DHT11** temperature sensor **characteristics** [3]: temperature determination in range of 0-50 °C with error deviation of 2°C, response frequency < 1 Hz, dimensions 15.5 x 12 x 5.5mm.

The NodeMCU V3 **ESP8266** transceiver **characteristics** [4]: protocols WiFi 802.11 b/g/n; built-in TCP/IP stack; digital and analog inputs D0-D8, SD1-SD3, AD0; power: 3.3-5V; power consumption: data exchange: 70 mA (200 mA maximum), standby time: <200 mA; board sizes 48x26mm; operating temperature -40...+125 °C.

To be able to send **temperature data** from the ESP8266 board, the necessary **program code** was created to program the ESP8266 board. Temperature data is written to relational **MySQL** to the Internet using **Web technologies (HTML, PHP)**. A web page based on **HTML & PHP** was created [5] to read data from database and visualize it (Fig. 3). The photo with students who implemented this project is shown on Fig. 3.

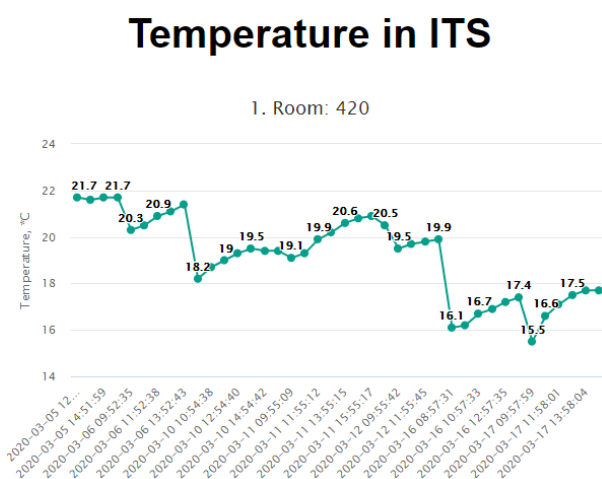


Fig. 3. The Web page with temperature data visualization in graph and students who implemented the project.

Thus, the IoT project is implemented for **automated** temperature collection, which **solves the task** of freeing human resources from **manual** temperature measurement. The 5 devices have been developed so far which are set up in the classrooms #403, 404, 406, 420, 503 of Telecommunication Systems Institute. Devices transmit temperature data values to MySQL database hourly, and data is visualized on the Web page [5]. The implemented IoT project allows a **flexible extension of devices number** to hundreds+, as well as allows devices extension by **other sensor types** (e.g., air quality, smoke, etc.).

References

1. IoT on Wikipedia https://en.wikipedia.org/wiki/Internet_of_things.
2. IoT Communication Technologies Guidebook <https://www.postscapes.com/internet-of-things-technologies/>
3. Sensor DHT11 <https://arduino.ua/prod185-datchik-vlajnosti-i-temperatyri-dht11>.
4. Transceiver ESP8266 <https://arduino.ua/prod1492-wi-fi-modul-nodemcu-esp8266>.
5. Visualization of the collected temperature data <http://its-temperature.radio-signal-telecom.in.ua/esp-charts-XX.php>.

TEMPERATURE MONITORING SYSTEM IN IOT NETWORK BASED ON ESP8266 MICROCONTROLLER AND THINGSPEAK SERVICE

Shevchuk A.O., Romanov O.I.

*Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: its.tk.kpi@ukr.net*

Система моніторингу температури в мережі IoT на базі мікроконтролеру ESP8266 та сервісу ThingSpeak

В роботі обговорюється проблеми підвищення температури в Україні та необхідність її моніторингу та використання технології Інтернет речей для контролю температури. Проаналізовано перспективи Інтернет речей в найближчі 25 років. Описано схему мережі системи моніторингу температури, її елементи та принцип роботи. Створена практична макетна модель на базі цифрового датчика температури, мікроконтролеру Node MCU ESP8266, вентилятору та сервісу ThingSpeak.

The rise in temperature in Ukraine and other countries due to global warming has led to an increase in the importance of monitoring the room temperature and maintaining it within acceptable room standards. As IoT (Internet of Things) is one of the most promising soon, it plays an important role in gathering information from sensors and transferring information to other devices that process the data received. Currently, the number of services that can analyze data is increasing. For example, services such as ThingSpeak, dweet.io, Blynk, and others.

It is expected that shortly IoT sensors will become active participants in our lives, where they will be able to exchange information and interact with each other without or through human intervention. To do this, they must respond autonomously to changes in the real world.

TechJury, a software company analyzing forecasts from various companies, predicts that by 2025, the number of devices connected to the Internet of Things will reach 64 billion. At the same time, marketing company Grand View Research predicts that the Internet of Things market will reach \$ 949.42 billion in the same year.

The steadily accelerated growth in the production of various types of sensors also speaks to the growth of the Internet of Things industry. Updating the hardware and software of sensors and systems based on them is happening at a rapid pace, and it is expected that in the next 25 years the size of the sensors will be significantly reduced, and sensors themselves will be even "smarter" and cheaper, which in turn will increase the scale of their use [1].

The system consists of the following elements:

- 1) temperature sensor DS18B20;
- 2) Node MCU ESP8266 microcontroller;
- 3) electric relay;
- 4) electric fan;
- 5) gateway (router);
- 6) ThingSpeak service;
- 7) computer with Internet access.

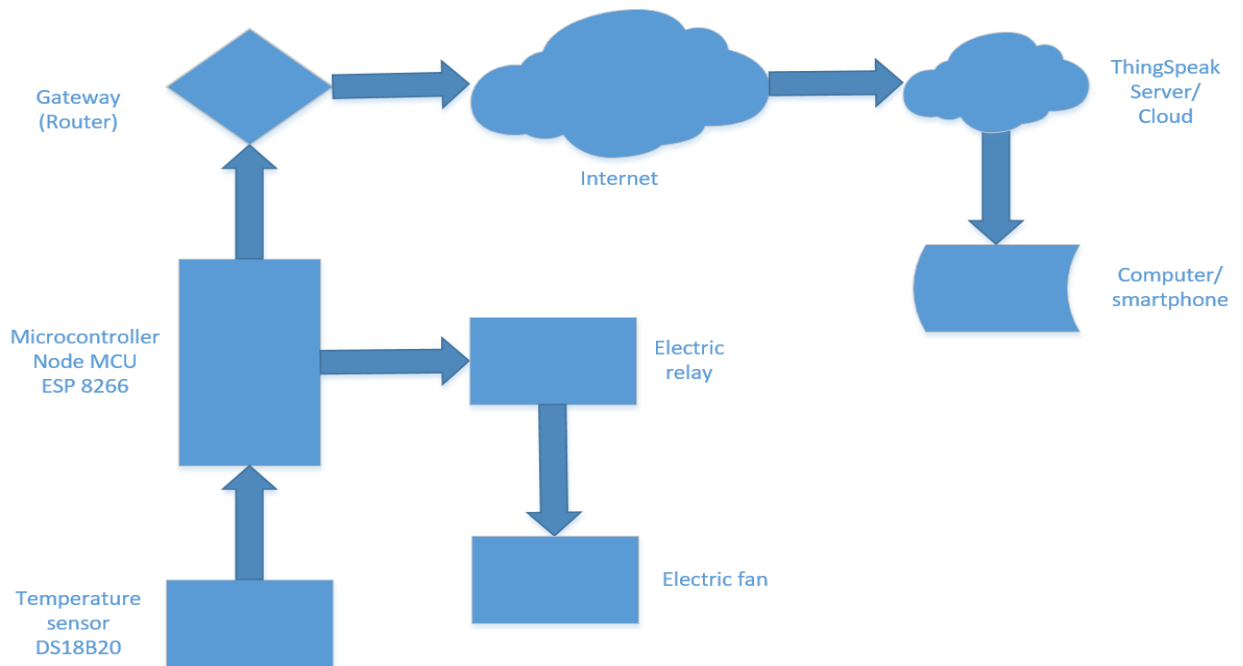


Figure 1. Block diagram of the system.

The principle of system operation is as follows. The digital DS18B20 sensor is read temperature. This sensor was selected because it has a sufficiently low measurement error, a large temperature range, and is powered by a voltage of 3.3 or 5B. Then signals are transmitted from the sensor using the 1-Wire protocol to the GPIO (General Purpose Input/Output) interface of the microcontroller with the Wi-Fi module Node MCU ESP8266 about temperature changes through the connecting wires.

A controller based on a written sketch in the Arduino IDE compares the temperature to the normal room temperature. If the temperature exceeds the threshold of normal temperature, a signal is transmitted from the microcontroller to the relay, which will switch contacts through the voltage supply and the fan will switch on. As soon as the temperature drops to normal, the fan shuts off.

The microcontroller then sends data from the Wi-Fi module through the gateway, in this case the home router via the Internet to the ThinkSpeak server.

Data from the sensor to the server is transmitted using the MQTT protocol.

The server collects and analyzes the data and builds a graph using Matlab based on that data. Finally, we have a graph that allows us to track temperature within a few thousand kilometers of sensors.

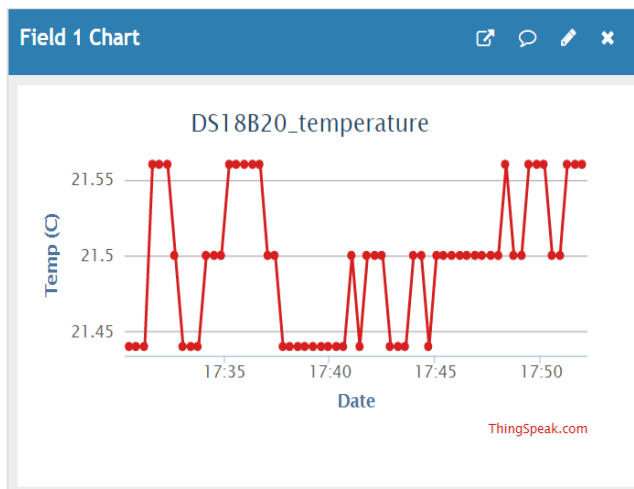


Figure 2. ThinkSpeak IoT Cloud Output result.

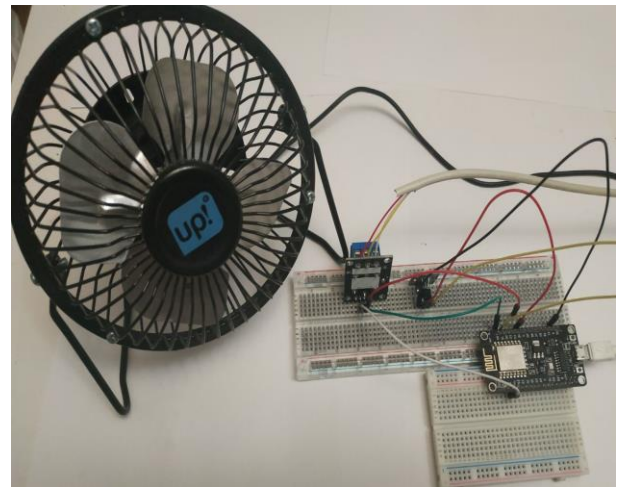


Figure 3. Hardware Setup.

Conclusion. To sum up everything, we can say that IoT will have a place. The Internet of Things will give us the ability to monitor temperature, humidity, water quality, air quality, and allow us to automate everything around us. This project can be scaled within the enterprise, the city using new data transfer technologies. In a few years, each house will have a smart fan, or air conditioning, or other appliances that will improve our lives.

References

1. Mr. R. Deekshath, Ms. P. Dharanya, Ms. K. R. Dimpil Kabadia, Mr. G. Deepak Dinakaran, "IoT Based Environmental Monitoring System using Arduino UNO and Thingspeak", International Journal of Science Technology & Engineering, 2349-784X, 2018.
2. Twinkle Gondaliya1, "Sensor communication in Smart Home Using IoT", International Institution for Technological Research and Development, 2016.
3. Атака «розумних» речей [Електронний ресурс: <http://nag.ru/articles/article/30371/ataka-umnyih-veschey.html>].
4. DS18B20 – датчик температуры с интерфейсом 1-Wire. Описание на русском языке. [<http://mypractic.ru/ds18b20-datchik-temperature-s-interfejsom-1-wire-opisanie-na-russkom-yazyke.html>].
5. Датчик температуры Arduino DS18B20 [<https://arduino-master.ru/datchiki-arduino/arduino-ds18b20/>].
6. DS18B20 Temperature Sensor with ESP8266 and ThingSpeak [<https://www.electronicshub.org/ds18b20-temperature-sensor-with-esp8266/>].
7. Khin Kyawt Kyawt Khaing, "Temperature and Humidity Monitoring and Control System with Thing Speak", International Journal of Scientific Research and Engineering Development, 2019.

METHOD OF MULTIPATH EFFECT ELIMINATION IN MOBILE COMMUNICATIONS

Uryvsky L.O., Solianikova V.Y.

*Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: leonid_uic@ukr.net, leka-br@mail.ru*

This article describes the multipath nature of radio waves propagation in space during transmission from the base station to the receiver and the effect on signal information forwarding. It also presents how to combat interference using OFDM technology.

Метод боротьби з багатопроменевістю в мобільному зв'язку

У даній статті описується багатопроменевий характер поширення радіохвиль у просторі при передачі від базової станції до приймача і його вплив на передачу сигналу. Описується спосіб боротьби з впливом інтерференції за допомогою технології OFDM.

The propagation of radio waves in free space, as a rule, depends on several factors, regardless of what radio communication is used for. Among the main factors, there are losses in free space, including receiver noise, additive interference, as well as multiplicative interference, the cause of which is the multipath nature of the propagation of electromagnetic waves that creates interference, i.e. superposition of waves in the receiver.

Apart from direct waves, the mobile receiver will receive some waves reflected from the surface of the Earth or other nearby objects (trees, stationary structures, etc.). Reflected waves with a random phase and amplitude are similar to the main wave, so they can cause some negative changes in the level of the main received signal. The longer the time delay of the reflected ray, the more interference appearance. Contrariwise, a delay significantly shorter than the signal duration is least manifested in reception quality.

Since it is difficult to influence the time delay, we can mitigate the effect of multiplicative noise by adaptively choosing the symbol duration of the transmitted signal, which is comparable (longer) with the time delay.

Thus, it is necessary to solve two problems:

- determine the method of adaptive change in the duration of the transmitted characters;
- estimate the delay time of the reflected rays.

As part of the first task, we note that in UMTS and LTE technologies, Orthogonal Frequency Division Multiplexing (OFDM) is used to transmit down-link streams. From the base station to the terminal, many narrow 180 kHz frequency bands are used for data transmission, instead of expanding one signal over the entire 5 MHz bandwidth, i.e. it uses a large number of narrow subcarriers for data transmission.

In order to solve the problem of the negative effects of multipath fading, OFDM technology is used to split a high-speed stream for one subscriber into a group of low-speed streams with orthogonal frequency division multiplexing. In each slow stream, the symbol durations will increase compared with the original stream by a number of times equal to the number of OFDM subcarriers. By controlling the number of subcarriers, we can control the duration of the transmitted characters.

To solve the second problem, let us look at the deterministic model of the VHF radio channel.

In [2], a mathematical model was proposed that gives a spatial description of the region of reflected rays formation by describing Cassini ovals.

A Cassini oval is a quartic plane curve defined as the set (or locus) of points in the plane such as the product of the distances to two fixed points (focus) is constant and equal to the square of a certain number a , i.e. $a^2 = R_1 R_2$.

Assuming that h_1, h_2 are the antenna heights, h_0 is the minimum effective antenna height, P_1 is the transmitter power, G_1 is the antenna gain, η_1 is the efficiency of the energy transmission system from the transmitter to the transmitting antenna, ω_{in} - receiver input resistance, U_{in} is the sensitivity of the receiver, it is possible to determine the region where the energy of the reflected signal exceeds the sensitivity of the receiver.

$$R_1 R_2 = \sqrt{(h_1^2 + h_0^2)(h_2^2 + h_0^2)} \sqrt{P_1 G_1 \eta_1 b_1 \eta_2 \omega_{BX} / U_{BX}} \quad (1)$$

Parameter b_1 – is the height of the obstacle located at a distance R_1 from the emitting station (radius of the first Fresnel zone), which can be determined by the dependence: $b_1 = \sqrt{(\lambda R / 3) r (1 - r)}$ (2), where R is the distance from the transmitting to the receiving antenna; r is the ratio of the distances to the obstacle and from the transmitting to the receiving antenna.

The parameter a depends on the characteristics of the communication system and soil characteristics included into the parameter h_0 . Marking half the distance between correspondents $R / 2 = c$, all cases of Cassini ovals can be reduced to the main ones: $a \geq c\sqrt{2}$; $c < a < c\sqrt{2}$; $a = c$; $0 < a < c$.

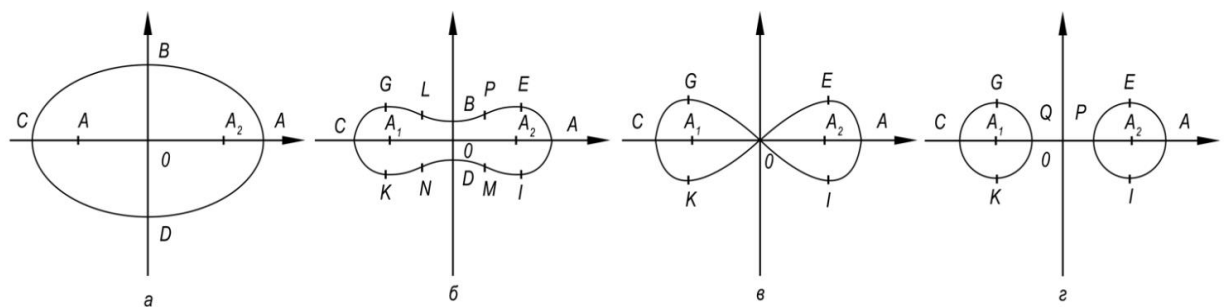


Fig. 1. Forms of zones formation of reflected rays.

In the first case, the Cassini oval is actually an oval with foci at the locations

of the receiving and transmitting stations (Fig. 2a). For $c < a < c\sqrt{2}$; the oval is more compressed in the middle of the route (Fig. 2b). In the third case, where $a = c$ - the reflection zone is a lemniscate (Fig. 2c). When $a < c$, the oval turns into circles around the locations of the antennas (Fig. 2d).

If we substitute the standard parameter values used in LTE into formula (1), we obtain certain parameter values a and c .

In the microwave range, signal transmission from the base station (point A) to the receiver (point A_I), which are located at a distance R , is illustrated in Fig. 3.

Suppose that the main signal passes from point A to point A_I , but at the same time another signal arrives at the receiver, reflected from the nearest surface. The voltage of the reflected signal exceeds the sensitivity of the receiver. Line A_I -C determines the radius of the reflection zone.

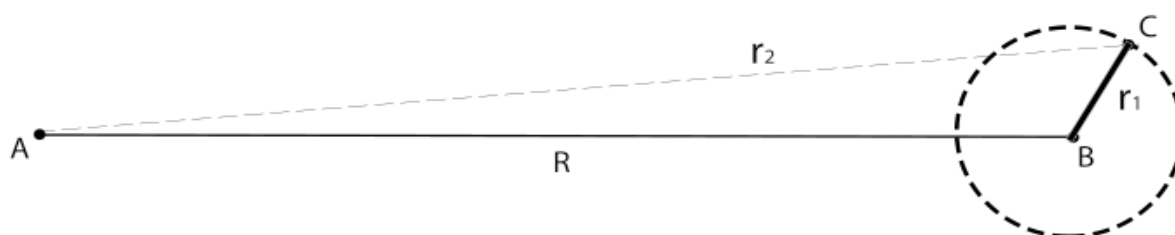


Fig. 2. Signal transmission from the base station to the receiver.

Using the initial parameters of the radio line, it is possible to calculate the diameter of the circle for the case of Fig. 2, $d: d = \sqrt{c^2 + a^2} - \sqrt{c^2 - a^2}$ (3)

and signal response delay: $\Delta t = \frac{d}{c}$ (4), where C is the speed of light.

The calculation of the response delay of the signal will give us the opportunity to compare this value with the duration of one character. Thus, a copy of the reflected previous signal (response) will not come superimposed on the adjacent signal. For this, it is necessary to increase the symbol duration by the time delay of its response by increasing the number of OFDM subcarriers in order to get rid of inter symbol interference.

Thus, OFDM technology will allow decomposing a high-speed data stream into a large number of substreams and transmitting each substream at a separate frequency, while increasing the length of the symbol. Obtaining spatial characteristics in a particular channel, it is possible to select such a number of subcarriers at which it is possible to minimize the influence of the multipath factor.

References

1. Abdollah Ghasemi, Ail Abedi, Farshid Ghasemi, "Propagation Engineering in Wireless Communication", Springer, 2012, pp. 247-249
2. Доровских А.В., Урывский Л.А., Луханин М.И. Способ распределения на местности ретрансляторов системы управления автомобильным транспортом /Автоматизация и механизация управления. - К.: УкрНИИ НТИ, № 1, 1985. - с.60...62.

SCOPES TO SOLVE PROBLEMS OF TELECOMMUNICATION RESOURCES DISTRIBUTION TO PROVIDE THE REQUIRED QoS

Martynova K.G.

*Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: scorpio.for.teen@gmail.com*

Можливості вирішення задачі розподілу телекомунікаційних ресурсів для забезпечення потрібного QoS

У статті розглядається задача розподілу телекомунікаційних ресурсів в межах уніфікованої системи масового обслуговування (СМО), що включає довільне число обслуговуючих приладів, місця для черги, а також різноманіття пріоритетів.

Multiservice systems are able to meet users' needs in storage and data processing that requires significant quantity of telecommunication resources: frequency, channels, time. General tendency shows that users choose the way of rising QoS requirements up. However, telecommunication resources are limited [1] and obviously the "fight" starts for the right to use these resources.

Thus, there is a problem of resources access that raises the number of tasks to solve for a telecommunication systems engineer. During the process of solving these tasks a specialist in telecommunications has to decide what should be "sacrificed" for all the users' sake.

Obviously, there is a huge variety of queuing systems (QS) intended for different kinds of tasks. In each case a telecommunication systems engineer encounters the analysis of quantitative and qualitative characteristics of QS aimed at choosing the most effective model.

The object of research is QS that consists of arbitrary number of streams and devices and various service disciplines.

Regardless of the QS type (see Figure 1), its structure is appropriate to be represented with following levels:

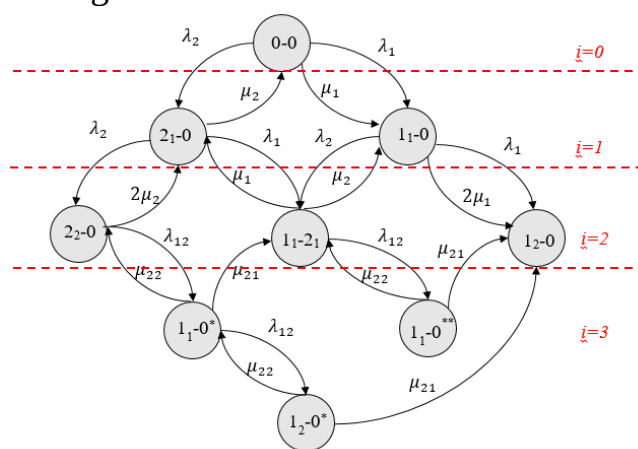


Figure. 2. The unified QS with two streams and to devices and queue [2].

- $i=0$: the system is free of requirements;
- $i=1$: the first device is occupied;
- $i=2$: the second device is occupied;
- $i=3$: requirements occupy the queue; the priority level (requirements “fight” for the place in queue).

To understand which role each level takes in dynamics of QS characteristics, let us formulate following questions.

1. How does the number of devices influence QoS characteristics?

Obviously, the easiest way to improve QoS characteristics is increasing the number of service devices.

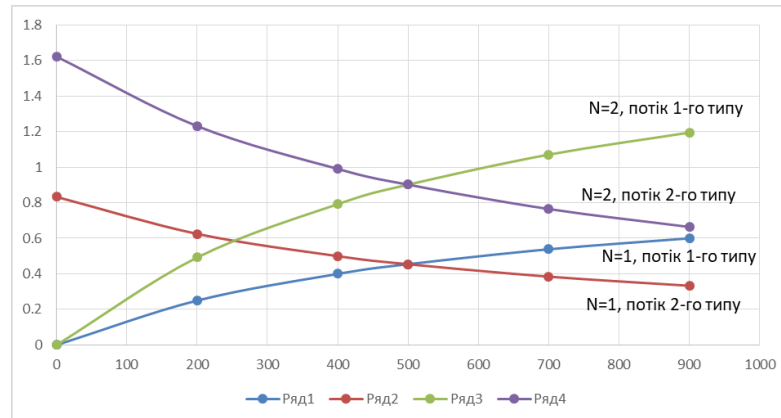


Figure 2. The dynamics of productivity characteristics with $N=1$ and $N=2$ depending on increasing of input load of the 1st type of requirements.

In Figure 2, there is a significant advantage in the characteristics of QS with two devices comparing to QS with one device. Undoubtedly, QS with two devices is capable to serve more requirements than QS with the only device. However, when it comes to dozens, hundreds of subscriber devices, the telecommunication service provider should think about the downtime probability of the system.

2. How does queue influence QoS characteristics?

In Figure 3, because of queues availability, there is a significant increase in productivity for the 1st type of requirements (20%), slightly less for the 2nd type of requirements - 12%. Increasing the number of servicing devices is a relatively more effective method of improving performance than queuing, but all of Little's criteria must be taken into account.

Along with the improvements made as the result of adding queue, there is an important problem for the user: a sharp increase of the average waiting time for service of the requirement. In QS models without queue, the requirements were either serviced or lost. The queue is a tool for reducing the number of lost requirements, but the improvement has to be “paid” in the time that the user spends on waiting.

3. How does the discipline of service influence QoS characteristics?

The discipline of service formally describes the service procedure (device occupation, waiting, service interruption) [1]. At the moment of the queue overflow, a choice of the appropriate for the current state of the QS, the discipline

of service becomes a panacea that provides the service of priority requirements and, if it is possible, applications of lower priority. The previous studies show [3], the use of priorities significantly improves QoS characteristics, relative priority in particular.

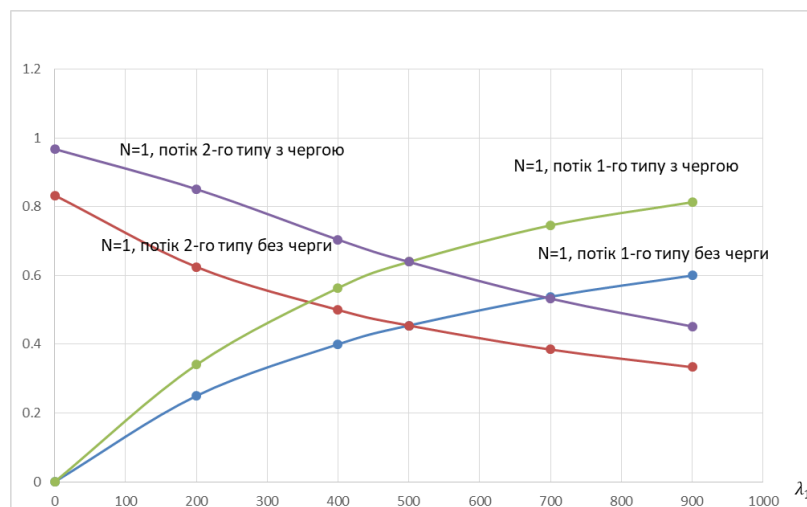


Figure 3. The dynamics of productivity characteristics with $N=1$, available queue and queue less depending on increasing of input load of the 1st type of requirements.

However, if the intensity of the input load is sharply increased, it is necessary to choose a discipline, depending on which of the available disciplines is the most optimal in the current state of QS. To do this, a telecommunication systems engineer must know the techniques of situational management.

Thus, having analyzed the observed problem and the number of questions that are able to highlight the problem, we conclude that increasing the number of servicing devices is suitable in case of QS with huge input loads. Adding queue is acceptable for QS with arbitrary input loads, but in this case, it is necessarily to take the average waiting time of requirements into account. Using the priority service is the most flexible tool for improvement QoS characteristics. At the same time, it is necessary to master the points of priority choice management in favor of this or another indicator of QoS characteristic [2].

References

1. Урывский Л.А. Обобщение процесса «размножение и гибели» на системы с «конфликтом доступа» // Наукові записки Українського науково-дослідного інституту зв'язку: науково-виробничий збірник. – 2009. – № 1. – с. 97-104.
2. Уривський Л.О., Гахова Г.С. Узагальнення системи масового обслуговування з пріоритетами //Тези доповіді/ IX Міжнародна НТК «Проблеми телекомунікацій», /Збірник матеріалів. — К.: ІТС НТУУ «КПІ», 2015, с. 77...79.
3. Уривський Л.О. Мартинова К.Г. Аналіз дисциплін обслуговування в мультисервісних телекомунікаційних системах// Тези доповіді/ XIII Міжнародна НТК «Перспективи телекомунікацій 2019», /Збірник матеріалів. — К.: ІТС НТУУ «КПІ», 2019, с. 1.



**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
"КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
ІМЕНІ ІГОРЯ СІКОРСЬКОГО"**

**ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ
НДІ ТЕЛЕКОМУНІКАЦІЙ**

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

Присвячено Дню науки та Всесвітньому Дню телекомунікацій

13–17 квітня 2020 року

Тези конференції

м. Київ

ПРОГРАМНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ ПРІТС-2020

Співголови конференції:

- ІЛЬЧЕНКО М.Ю. – науковий керівник, директор Інституту телекомунікаційних систем Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», академік НАНУ, д.т.н., професор;
- ЯКОРНОВ Є.А. – к.т.н., професор Інституту телекомунікаційних систем КПІ ім. Ігоря Сікорського;
- ГАНЖА Я.В. – голова студентської Ради Інституту телекомунікаційних систем КПІ ім. Ігоря Сікорського.

Члени наглядового комітету:

- ГЛОБА Л.С. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
КОНОНОВА І.В. – к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
КРАВЧУК С.О. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
ЛИСЕНКО О.І. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
МАКСИМОВ В.В. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
МІНОЧКІН Д.А. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
МОШИНСЬКА А.В. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
НАРИТНИК Т.М. - к.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
ПРАВИЛО В.В. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
РОМАНОВ О.І. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
СКУЛИШ М.А. - д.т.н., с.н.с., КПІ ім. Ігоря Сікорського, Київ;
ТРУБАРОВ І.В. – к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
ТРУБІН О.О. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
УРИВСЬКИЙ Л.О. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
ШЕЛКОВНИКОВ Б.М. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
ЯВІСЯ В.С. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ.

Члени програмного комітету:

- Авдеєнко Г.Л., ст. викладач, КПІ ім. Ігоря Сікорського, ІТС, Київ;
Афанасьєва Л.О., асистент каф. ТК, КПІ ім. Ігоря Сікорського, ІТС, Київ;
Валуїський С.В., к.т.н., доц., КПІ ім. Ігоря Сікорського, ІТС, Київ;
Кравчук І.М., ст. викладач, КПІ ім. Ігоря Сікорського, ІТС, Київ;
Курдеча В.В., ст. викладач, КПІ ім. Ігоря Сікорського, ІТС, Київ;
Новіков В.О., ст. викладач, КПІ ім. Ігоря Сікорського, ІТС, Київ;
Штогриня О.С., к.т.н., КПІ ім. Ігоря Сікорського, ІТС, Київ.

Засідання 1.

АВТОКОМПЕНСАТОР ЗАВАД ДЛЯ ПРИЙМАЧІВ РАДІОРЕЛЕЙНОГО ЗВ'ЯЗКУ

Москалюк С.О.

Науковий керівник: **Якорнов Є.А.**

Інститут телекомунікаційних систем

КПІ ім. Ігоря Сікорського, Україна

E-mail: sviatoslav.moskaliuk@gmail.com

Сформульовано підхід до створення автокомпенсатора перешкод з придушенням до 80 дБ. В якості перешкоди для приймача одночастотної лінії радіорелейного зв'язку виступає сигнал свого передавача.

INTERFERENCE AUTOCOMPENSATOR FOR RADIO RELAY RECEIVERS

Moskaliuk S.O.

Scientific adviser: **Yakornov Y.A.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: sviatoslav.moskaliuk@gmail.com

The approach to the creation of an interference compensator with 80 dB suppression is formulated. As a barrier to the receiver of a single-frequency line relay communication is the signal of his transmitter.

РОЛЬ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ПРОЦЕССЕ ВЫРАЩИВАНИЯ ПРОДУКТОВ ПИТАНИЯ

Нидченко И. А.

Науковий керівник: **Лысенко А. И.**

Інститут телекомунікаційних систем,

КПІ ім. Ігоря Сікорського, Україна

E-mail: nidchenkoilya@gmail.com

Частая культивация и использование земли приводит к истощению почвы. Все большую популярность приобретают продукты, выращенные без применения или с минимальным применением удобрений и химикатов. Предложено альтернативный метод выращивания органической продукции. Проведено анализ требуемых факторов мониторинга за органикой.

THE ROLE OF TELECOMMUNICATION-INFORMATION TECHNOLOGIES IN THE PROCESS OF GROWING FOOD

Nidchenko I. A.

Scientific adviser: **Lysenko. A. I.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: nidchenkoilya@gmail.com

Frequent cultivation and land use leads to soil depletion. Products grown without or with minimal use of fertilizers and chemicals are becoming increasingly popular. An alternative method of growing organic products is proposed. The analysis of the required factors for monitoring organic plants is carried out.

АНАЛІЗ ПРОТОКОЛУ DATA DISTRIBUTION SERVICE (DDS)

Нсер А.М.

Науковий консультант: **Рибак О.О.**

Інститут телекомунікаційних систем,

КПІ ім. Ігоря Сікорського, Україна

E-mail: anzhela.nser.angel@gmail.com

Досліджено особливості протоколу проміжного програмного забезпечення та стандарту міжмашинної взаємодії Data Distribution Service (DDS). Даний протокол відіграє ключову роль в напрямку інтернет речей та ідеально підходить для додатків, яким потрібна довговічна, надійна і високопродуктивна архітектура. Було проведено порівняльну характеристику DDS з подібними протоколами.

PROTOCOL ANALYSIS DATA DISTRIBUTION SERVICE(DDS)

Nser A.M.

Scientific consultant: **Rybak O.O.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: anzhela.nser.angel@gmail.com

The features of the middleware protocol and the interoperability standard are investigated which is Data Distribution Service (DDS). This protocol is a key role in the Internet of Things and is ideally suited for applications that need a durable, reliable and high-performance architecture. A comparative characterization of DDS was performed with similar protocols.

АНАЛІЗ РОЗВИТКУ ТЕХНОЛОГІЇ 5-ГО ПОКОЛІННЯ В УКРАЇНІ

Корман Н.А

Науковий керівник: **Могилевич Д.І.**
Інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: kormannatasha21292@gmail.com

Проведено аналіз розвитку технології 5-го покоління на території України. Технологія 5G дозволять активне з'єднання до 1 мільйону пристроїв на один квадратний кілометр та має швидкість, що перевищує 4G у 20 разів.

Технологію 5-го покоління має ряд важливих переваг: вища пропускна здатність, доступність широкосмугового мобільного зв'язку, використання режимів device-to-device, наднадійні масштабні системи комунікації, більш короткий час затримки, мінімальні витрати енергії батарей.

Розглядаючи питання впровадження технології 5G в Україні, можна зіткнутись з рядом проблем: частоти, які можуть бути використані під технології п'ятого покоління, особливості розгортання, неготовність абонентів.

Предметом подальших досліджень є системи мобільного зв'язку, які постійно розвиваються та удосконалюються, а також розробка технології "Інтернет речей", щоб повністю замінити Wi-Fi обладнання, яке не прив'язуватиме абонента до точки доступу з обмеженим радіусом дії на території України.

ANALYSIS OF TECHNOLOGY DEVELOPMENT OF THE 5TH GENERATION IN UKRAINE

Korman N.A

Scientific adviser: **Mogilevich D.I.**
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: kormannatasha21292@gmail.com

The analysis of the development of technology of the 5th generation in the territory of Ukraine is conducted. 5G technology will allow up to 1 million devices per square kilometer to be actively connected and has a speed exceeding 4G by 20 times.

5G has a number of important benefits: higher bandwidth, broadband mobile availability, device-to-device modes, high-reliability large-scale communication systems, shorter latency, and minimal battery life.

When considering the introduction of 5G technology in Ukraine, you may encounter a number of problems: frequencies that can be used for fifth-generation technologies, deployment features, unpreparedness of subscribers.

The subject of further research is mobile systems that are constantly evolving and improving, as well as the development of "Internet of Things" technology to completely replace Wi-Fi equipment, which will not tie the subscriber to a restricted access point in Ukraine.

АНАЛІЗ ОСНОВНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

Турчин Я. В.

Науковий керівник: **Кононова І.В.**

Інститут телекомунікаційних систем

КПІ ім. Ігоря Сікорського, Україна

E-mail: turchyn_v@ukr.net

Проведено аналіз основних методів захисту інформації від несанкціонованого доступу або спотворення. Визначено найкращих способ збереження цілісності та достовірності даних. Швидкий стрибок у розвитку комп'ютерних технологій в автоматизованих системах обробки та управління інформації, запровадив нові вимоги для забезпечення захисту. Серед усього спектру методів захисту інформації від небажаного доступу особливе місце займають криптографічні методи. Вони дають можливість розподілу ресурсів мережі, якщо виникають проблеми з працездатністю окремих елементів, підтвердження достовірності об'єктів та захисту програмних продуктів. Тому, необхідність використання криптографічних систем зростає з кожним днем. Як наслідок, виняткову практичність набуває питання про методи і критерії оцінки безпеки інформаційних систем.

На сьогоднішній день криптографічні методи – одна з найважливіших частин усіх інформаційних систем: від електронної пошти до мобільного зв'язку та від доступу до мережі Інтернет до електронної готівки. Використання саме цих методів може забезпечити прозорість, точність і конфіденційність інформаційних даних.

ANALYSIS OF THE BASIC METHODS OF INFORMATION PROTECTION

Turchyn Y.V.

Scientific adviser: **Kononova I.V.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: turchyn_v@ukr.net

The basic methods of protection of information from unauthorized access or distortion are analyzed. The best way to preserve the integrity and reliability of your data is identified. The rapid leap in the development of computer technology in automated information processing and management systems has introduced new security requirements. Cryptographic methods have a special place in the whole spectrum of methods of protecting information against unwanted access. They allow you to allocate network resources if you have problems with the performance of individual elements, validation of objects and protection of software. Therefore, the need to use cryptographic systems is increasing day by day. As a consequence, the question of methods and criteria for assessing the security of information systems becomes extremely practical.

Today, cryptographic methods are one of the most important parts of all information systems: from e-mail to mobile communication and from access to the Internet to electronic cash. Using these methods can ensure transparency, accuracy and confidentiality of information.

ОСОБЛИВОСТІ ТЕХНОЛОГІЇ REST API В ІoT

Безвугляк М.С.

Науковий керівник: **Курдеча В.В.**

Інститут телекомунікаційних систем,

КПІ ім. Ігоря Сікорського, Україна

E-mail: maximbezvugliak@gmail.com

На сьогоднішній день у світі телекомунікацій та в Інтернет речей зокрема існує проблема захисту інформації. Подоланню цієї проблеми присвячено значна кількість наукових праць вітчизняних та світових вчених. В даній роботі запропоновано застосування REST API дозволяє підвищити безпеку запитів і тому є доцільним для застосування в Інтернеті речей. В роботі визначено особливості, які необхідно врахувати для застосування REST API, сформовано перелік вимог для його впровадження. Також проведено оцінку позитивного ефекту від впровадження даної технології.

FEATURES OF REST API TECHNOLOGY IN IoT

Bezvuhiak M.S.

Scientific adviser: **Kurdecha V.V.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: maximbezvugliak@gmail.com

Today, in the world of telecommunications and the Internet of Things, in particular, there is the problem of protecting information. A considerable amount of scientific works of national and world scientists is devoted to overcoming this problem. In this paper, the proposed application of the REST API allows to increase the security of requests and is therefore appropriate for use on the Internet of Things. The paper defines the features that must be considered for the application of the REST API, and a list of requirements for its implementation. The positive effect of this technology was also evaluated.

АНАЛІЗ ЗАГРОЗ ОСНОВНИХ КОМПОНЕНТІВ ІОТ

Піхота К. В.

Науковий керівник: **Кононова І.В.**

Інститут телекомунікаційних систем,

КПІ ім. Ігоря Сікорського, Україна

E-mail: pihotka19.11@gmail.com

На сьогоднішній день прилади і системи ІоТ уже неодноразово зазнавали атак, тому забезпечення їх захисту є одним з ключових завдань.

Розглядаючи основні компоненти ІоТ можна виділити такі технології: RFID, NFC та WSNs. Най вразливішою з них є NFC (загроза прослуховування та атаки відмови в обслуговуванні(DoS)). В RFID-системі виникають загрози десинхронізації, витік інформації та повторення атак. WSNs є вразливими до різних видів атак майже на всіх рівнях стеку протоколів.

Для захисту від втручання в код програми та підміни показників датчиків слід використовувати технологію блокчейн. Блокчейн дозволить відстежувати вимірювання даних сенсора та запобігання дублюванню шкідливими даними, а також забезпечить автентифікацію та безпечну передачу даних.

ANALYSIS OF THREATS TO THE MAIN COMPONENTS OF THE IoT

Pikhota K.V.

Scientific adviser: **Kononova I.V.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: pihotka19.11@gmail.com

Today, the devices and systems of the IoT have already been attacked many times, so ensuring their protection is one of the key tasks.

Considering the main components of the IoT, the following technologies can be distinguished: RFID, NFC and WSNs. The most vulnerable of these is NFC (listening threat and Denial of Service (DoS) attack). The RFID system has threats of desynchronization, information leakage, and repetition of attacks. WSNs are vulnerable to various types of attacks at almost all levels of the protocol stack.

Blockchain technology should be used to protect against program code interference and sensor offenses. Blockchain will allow to monitor sensor data measurement and avoid harmful data duplication, as well as provide authentication and secure data transmission.

СИСТЕМА УПРАВЛІННЯ МЕРЕЖЕЮ MICROGRID

Волчан Д.В.

Науковий керівник: **Курдеча В.В.**

Інститут телекомунікаційних систем

КПІ ім. Ігоря Сікорського, Україна

E-mail: dimon259.259@gmail.com

Існує багато різних способів управління мережею MicroGrid. У цій роботі розглядаються існуючі методи управління мережею MicroGrid та висвітлюється важливість стратегій управління енергією. Зазвичай управління мережею MicroGrid формується як проблема оптимізації в режимі офлайн. Більшість цих методів являють собою чітке прогнозування відновлюваних джерел енергії, потреб та ринку, що в дійсності спрогнозувати досить непросто. Ця робота зосереджується на розробці онлайн-стратегії управління енергією для роботи MicroGrid у режимі реального часу, яка враховує потік електроенергії та експлуатаційні обмеження системи в розподільній мережі.

MICROGRID NETWORK MANAGEMENT SYSTEM

Dmytro Volchan

Scientific adviser: **Vasyl Kurdecha**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: dimon259.259@gmail.com

There are many different ways to manage your MicroGrid network. This paper reviews existing MicroGrid network management practices and highlights the importance of energy management strategies. Typically, MicroGrid network management is shaped as an offline optimization problem. Most of these methods are clear forecasts of renewable energy, needs and markets, which is not easy to predict. This focuses on developing a real-time online energy management strategy for MicroGrid that takes into account electricity flow and system operating constraints on the distribution network.

ПЕРСПЕКТИВИ РОЗВИТКУ ІНТЕРНЕТУ РЕЧЕЙ

Карлін П.Ю.

Науковий керівник: **Курдеча В.В.**

Інститут телекомунікаційних систем,

КПІ ім. Ігоря Сікорського, Україна

E-mail: pashakarlin1234@gmail.com

Робота присвячена аналізу тенденції розвитку інтернету речей. Завдяки аналізу перспектив розвитку IoT (Internet of Things), виявлено потенціальні проблеми, пов'язані з майбутніми DDOS-атаками, на шляху розвитку та прогресивного впровадження технологій інтернету речей, відслідковано тенденцію зросту кількості користувачів даної технології.

PROSPECTS OF DEVELOPMENT OF THE INTERNET OF THINGS

Karlin P.Y.

Scientific adviser: **Kurdecha V.V.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: pashakarlin1234@gmail.com

The work is devoted to the analysis of the tendency of development of the Internet of Things. Analyzing the prospects for the development of IoT (Internet of Things), identified potential problems associated with future DDOS attacks in the path of development and progressive introduction of Internet of Things technology, and monitored the trend of growth in the number of users of this technology.

МЕХАНІЗМ ПЕРЕНЕСЕННЯ АКТИВНОГО З'ЄДНАННЯ МІЖ КАНАЛАМИ ЗВ'ЯЗКУ МОБІЛЬНОЇ МЕРЕЖІ

Ловеїкін Д.Ю.

Науковий керівник: **Носков В.І.**

Інститут телекомунікаційних систем,

КПІ ім. Ігоря Сікорського, Україна

E-mail: danylo275@gmail.com

В даній роботі розглянуто основні принципи забезпечення безперервного з'єднання абонентського терміналу з базовими станціями в умовах руху за допомогою хендверів в мережі мобільного зв'язку.

Також розглядаються основні проблеми, які з'являються під час перемикання на сусідню базову станцію, шляхи їх вирішення та оптимізації.

THE MECHANISM OF TRANSFERRING AN ACTIVE CONNECTION BETWEEN COMMUNICATION CHANNELS FOR MOBILE NETWORK

Loveikin D.Y.

Scientific adviser: **Noskov V.I.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: danylo275@gmail.com

The basic principles of continuous connection providing between user terminal and base stations using handovers under moving conditions were considered in this work.

Also, the main problems that appear during the switching process to the neighbour base station and the ways to resolve these problems were investigated.

КОМПЛЕКСНА АНАЛІТИЧНА МОДЕЛЬ ОБСЛУГОВУВАННЯ НА ХМАРНОМУ СЕРВЕРІ ПОВІДОМЛЕНЬ ІЗ ОЗНАКАМИ ПРІОРИТЕТІВ

Мартінова К.Г.

Науковий керівник: **Уривський Л.О.**

Інститут телекомунікаційних систем,

КПІ ім. Ігоря Сікорського, Україна

E-mail: scorpio.for.teen@gmail.com

У доповіді розглядається проблема розподілу телекомунікаційних ресурсів в межах уніфікованої багатопріоритетної системи масового обслуговування (СМО), що включає довільне число обслуговуючих приладів, місця для черги, а також різноманіття пріоритетів. Хмарний сервер виступає засобом обробки заявок (електронним обчислювальним ресурсом). Показані залежності показників якості обслуговування (QoS) від інструментів впливу на QoS (прилади, черга, дисципліни обслуговування). Пропонується комплексна аналітична модель, що відповідає розглянутим системам масового обслуговування. Доведено, що отриманий математичний апарат задовольняє описаним моделям СМО.

COMPLEX ANALYTICAL MODEL OF REQUIRES SERVICE WITH PRIORITY ATTRIBUTES ON CLOUD SERVER

Martynova K.G.

Scientific adviser: **Uryvsky L.O.**

Institute of telecommunication systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: scorpio.for.teen@gmail.com

The report, observes the problem of distributing telecommunication resources in the unified queuing system (QS), which includes the number of devices, queue, and the variety of priorities. The cloud server is the mean of request service (an electronic resource). Dependences of quality of service (QoS) characteristics on influence tools such as number of devices, queue and disciplines of service are shown. The complex analytical model, which is acceptable for mentioned queuing systems. It is proved that the obtained mathematical formula satisfies described models of QS.

ЗАСТОСУВАННЯ КОНЦЕПЦІЇ DATA BANK В МЕРЕЖІ ХМАРНОГО IoT

Пороло Є.О.

Науковий керівник: **Курдеча В.В.**

Інститут телекомунікаційних систем,

КПІ ім. Ігоря Сікорського, Україна

E-mail: jeykeuwork@gmail.com

За оцінками експертів зростає кількість користувачів Інтернет, кількість вузлів міжмашинного обміну інформації та об'єм передаваних даних. А тому з'явилась тенденція, за якої користувачі оплачують інформаційні послуги за рахунок доступу до своїх даних та відповідної їх статистичної обробки. Використання концепції DataBank дозволить користувачам контролювати свої дані, що будуть передаватися до постачальників послуг. В роботі проведено огляд існуючих рішень та проблем контролю даних. Запропоновано модифіковану архітектуру Інтернету речей за рахунок застосування технології DataBank для збереження конфіденційності в процесі збору та обміну даними.

DATA BANK CONCEPT ON CLOUD IoT

Porolo Y.O.

Scientific adviser: **Kurdecha V.V.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: jeykeuwork@gmail.com

According to experts, the number of Internet users and inter-machine data exchange nodes and the amount of data transmitted are increasing. Therefore, there is a tendency for users to pay for information services through access to their data and their corresponding statistical processing. Using the Data Bank concept will allow users to control their data that will be transferred to service providers. The paper reviews existing solutions and problems of data control. A modified Internet of Things architecture is proposed through the use of Data Bank technology to maintain confidentiality in data collection and sharing.

ЗАСТОСУВАННЯ PROTOBUF В ІНДУСТРІАЛЬНОМУ ІНТЕРНЕТІ РЕЧЕЙ

Попенко Д.В.

Науковий керівник: **Курдеча В.В.**

Інститут телекомунікаційних систем,

КПІ ім. Ігоря Сікорського, Україна

E-mail: demyd.popenko@gmail.com

Через розвиток автоматизації та впровадження Індустріального Інтернету речей стає можливим збір інформації, який дозволяє керівництву отримувати об'єктивні і точні дані про стан виробництва. Отримані з датчиків та контролерів неоднорідні структури даних необхідно серіалізувати, тобто перетворювати в бітову послідовність і передавати по мережі. В роботі проаналізовано існуючі методи серіалізації та проведено оцінку за критерієм часу. Найкращий результат отримано використовуючи метод Protobuf, оскільки він використовує строгу типізацію полів і бінарний формат для передачі структурованих даних. Через це система витрачає менше ресурсів, що є важливим для швидкого отримання точних даних.

PROTOBUF APPLICATION ON INDUSTRIAL INTERNET OF THINGS

Popenko D.V.

Scientific adviser: **Kurdecha V.V.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: demyd.popenko@gmail.com

With the development of automation and the introduction of the Industrial Internet of Things, it is possible to collect information that allows management to obtain objective and accurate data on the state of production. The heterogeneous data structures obtained from the sensors and controllers must be serialized, i.e. converted into a bit sequence and transmitted over the network. The paper analyzed existing serialization methods and conducted evaluation by time criterion. The best result was obtained using the Protobuf method, as it uses strongly typed fields and binary format to transmit structured data. As a result, the system consumes less resources, which is important for quickly obtaining accurate data.

ПІДХІД ДО ДОСЛІДЖЕННЯ ПСИХОФІЗІОЛОГІЧНОГО СТАНУ ЛЮДИНИ НА ОСНОВІ КОЛЬОРОВОЇ ПРЕФЕРЕНЦІЇ ТА СУБ'ЄКТИВНИХ ВІДЧУТТІВ

Копя Р.В.

Науковий керівник: **Штогріна О. С.**

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: roma.kpv@gmail.com

На сьогоднішній день знаходження факторів, які впливають на стан людини, займає багато часу, оскільки потребує обробки великої кількості результатів тестів, а також визначення закономірностей та пошуку залежностей між ними. З метою підвищення ефективності знаходження факторів впливу на стан людини було запропоновано підхід до дослідження психофізіологічного стану людини на основі кольорової преференції який дозволяє встановити взаємозв'язок між суб'єктивним відчуттям людини та кольоровою преференцією. Вищезгаданий підхід до дослідження психофізіологічного стану людини дозволить спростити роботу психологів та працівників Національного антарктичного наукового центру.

APPROACH TO THE INVESTIGATION OF THE PSYCHOPHYSIOLOGICAL STATE OF HUMAN BASED ON COLOR PREFERENCE AND SUBJECT FEELINGS

Kopya R.V.

Scientific adviser: **Shtogrina O.S.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: roma.kpv@gmail.com

To date, finding the factors that affect a person's condition is time-consuming, since it requires processing a large number of test results, as well as identifying patterns and finding relationships between them. In order to increase the effectiveness of finding the factors of influence on the human condition, an approach was proposed to study the psychophysiological state of a person based on color preference, which allows to establish the relationship between subjective human feeling and color preference. The aforementioned approach to the study of the psychophysiological state of man will allow to simplify the work of psychologists and employees of the National Antarctic Science Center.

Засідання 2.

МЕТОД ЗБОРУ ТА ОБРОБКИ ІНФОРМАЦІЇ В МЕРЕЖІ MICROGRID

Степанов Г. О.

Науковий керівник: **Курдеча В. В.**

Інститут телекомунікаційних систем,

КПІ ім. Ігоря Сікорського

E-mail: glib4400@gmail.com

Мережі Microgrid швидкими темпами набирають популярність, а отже постає питання зручності використання нинішніх методів збору та обробки інформації.

Споживачі матимуть можливість оцінювати спожиту енергію та на основі отриманої інформації та адаптувати витрати на електроенергію.

Також у розумних будинках клієнтів інтелектуальні пристрої генерують інформацію яка надсилається на розумні лічильники та використовується Microgrid для забезпечення балансу.

У даній роботі запропонований модифікований метод збору інформації з датчиків, обладнання та інтелектуальних пристроїв по всій мережі, з передачею на контролер для зберігання та обробки.

METHOD OF COLLECTING AND PROCESSING INFORMATION ON A MICROGRID NETWORK

Stepanov G. O.

Scientific adviser: **Kurdecha V. V.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: glib4400@gmail.com

Microgrid networks are gaining momentum, and so there is the question of the convenience of using current methods of gathering and processing information.

Consumers will be able to evaluate the energy consumed and on the basis of the information received and adjust the energy costs.

Also in smart homes, smart devices generate information that is sent to smart meters and used by Microgrid to maintain balance.

This paper proposes a modified method of collecting information from sensors, equipment, and smart devices across the network, with transmission to a controller for storage and processing.

ПЕРСПЕКТИВА ВИКОРИСТАННЯ ІНТЕРНЕТ РЕЧЕЙ В КОНЦЕПЦІЇ “ЯКРАЗ ВЧАСНО”

Берлоус В.О.

Науковий керівник: **Курдеча В. В.**

Інститут телекомунікаційних систем

КПІ ім. Ігоря Сікорського, Україна

E-mail: McFord@ukr.net

Згідно статистичних даних зростає кількість вузлів Інтернет речей, так вводяться нові сфери застосування IoT-пристроїв та об'єм передавальної інформації. Досліджено концепцію системи виробництва “якраз вчасно” та роль Інтернету речей в ній, на прикладі автозаводу. Проаналізована подальша перспектива використання Інтернет речей на виробництві у напрямку створення саморегулюючої системи з мінімальним або взагалі відсутнім втручанням людини у виробничий процес.

PERSPECTIVE OF USING INTERNET OF THINGS IN JUST-IN-TIME

Berlous V.O.

Scientific adviser: **Kurdecha V. V.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: McFord@ukr.net

According to statistics, the number of Internet of Things nodes is growing, new scopes of IoT devices are being introduced and the amount of information being transferred. Investigated of the conception of Just-In-Time (JIT) and Internet of Things (IoT) role in JIT on example automobile factory. Analyzed the perspective using IoT in production industry, namely create of self-regulation system with minimal or without human intervention in production process.

ІНФОРМАЦІЙНА БЕЗПЕКА INTERNET OF THINGS

Петров О.С.

Науковий керівник: **Курдеча В.В.**

Інститут телекомунікаційних систем,

КПІ ім. Ігоря Сікорського, Україна

E-mail: alexashka010100@gmail.com

Робота присвячена інформаційній безпеці Інтернету речей. Досліджено проблеми інформаційної безпеки Інтернету речей і безпосередньо розглянуто поняття безпеки в IoT. Запропоновано модифікацію архітектури Інтернету речей. Виділено і класифіковано можливі і найбільш вірогідні джерела виникнення небезпеки. Проаналізовано причини та передумови виникнення загроз та запропоновано первинні способи вирішення та їх запобігання.

INTERNET OF THINGS INFORMATION SECURITY

Petrov O.S.

Scientific adviser: **Kurdecha V.V.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: alexashka010100@gmail.com

The work is devoted to information security of the Internet of Things. Investigated the problems of information security of the Internet of Things and directly considered the concept of security in IoT. Proposed a modification of the Internet of Things architecture. Identified and classified the possible and the most likely sources of danger. Analyzed the causes and prerequisites of the threats and suggested the initial solutions and their prevention.

ДОСЛІДЖЕННЯ ВПЛИВУ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ НА НАДІЙНІСТЬ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

Вітковський В.І.

Науковий керівник: **Гаттуров В.К.**

Інститут телекомунікаційних систем,

КПІ ім. Ігоря Сікорського, Україна

E-mail: kortesswork@gmail.com

У статті досліджено принципи побудови мережевого провайдера, організації рівнів мережевої архітектури та визначення топології для цих рівнів. Також проводиться аналітика оцінки впливів вибраної топології та протоколів маршрутизації на надійність мережевого з'єднання після надзвичайної ситуації.

INVESTIGATION OF THE INFLUENCE OF ROUTING PROTOCOLS ON THE RELIABILITY OF THE TELECOMMUNICATIONS NETWORK

Vitkovsky V.I.

Scientific adviser: **Gatturov V.K.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: kortesswork@gmail.com

This article describes the principles for building a network provider, organizing levels of network architecture, and determining the topology for those levels. The article describes how to evaluate the impact of the selected topology and routing protocols on the reliability of the network connection after an emergency.

**ДОСЛІДЖЕННЯ СЦЕНАРІЇВ ВЗАЄМОДІЇ
ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ЗКС-7 З МЕРЕЖАМИ
НАСТУПНОГО ПОКОЛІННЯ НА БАЗІ IMS**

Мещерінов М.В.

Науковий керівник : **Гаттуров В. К.**

Інститут телекомунікаційних систем,

КПІ ім. Ігоря Сікорського, Україна

E-mail: mmieshch@gmail.com

Проведено аналітичне дослідження можливості використання технології ЗКС-7 в мережі наступного покоління завдяки впровадженню концепції IMS в мобільні мережі.

**RESEARCH OF SCENARIOS OF INTERACTION OF
TELECOMMUNICATION NETWORKS SS-7 WITH
NEXT GENERATION NETWORKS BASED ON IMS**

Mieshcherinov M.V.

Scientific adviser: **Gatturov V.K.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: mmieshch@gmail.com

This article examines the use of SS7 technology in next generation network through the implementation of the IMS concept into mobile networks.

МЕТОДИ ЗМЕНШЕННЯ РІВНЯ ІНТЕРФЕРЕНЦІЇ ВІД ЗАСТОСУВАННЯ РАДІО ПОВТОРЮВАЧІВ В МЕРЕЖАХ UMTS

Скрябін С.А.

Науковий керівник: **Носков В.І.**

Інститут телекомунікаційних систем,

КПІ ім. Ігоря Сікорського, Україна

E-mail: sergiy.skriabin@ukr.net

Було з'ясовано принцип дії та складові частини радіо повторювача. Крім того, розглянуто причини погіршення якості покриття мережі мобільного зв'язку, які роблять необхідним використання радіо ретрансляторів. Розглянуті варіанти підвищення якості мобільного зв'язку, через зменшення рівня інтерференції, від застосування радіо повторювачів.

METHODS OF REDUCING THE INTERFERENCE LEVEL FROM THE APPLICATION OF RADIO REPEATERS WITHIN UMTS NETWORKS

Skriabin S.A.

Scientific adviser: **Noskov V.I.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: sergiy.skriabin@ukr.net

The principle of operation and components of the radio repeater were clarified. In addition, the reasons for the deterioration in the quality of coverage of the mobile network that make the use of radio repeaters were investigated. Options for improving the quality of mobile communication due to the decrease in the level of interference from the use of radio repeaters were considered.

РОЗГОРТАННЯ SDN В КОРПОРАТИВНИХ МЕРЕЖАХ НА БАЗІ КОНТРОЛЕРА APIC-ЕМ ФІРМИ CISCO

Пявчик М.О.

Науковий керівник: **Григоренко О.Г.**

Інститут телекомунікаційних систем,

КПІ ім. Ігоря Сікорського, Україна

E-mail: max140699@gmail.com

Розглянуто призначення та особливості технології SDN. Ефективність та переваги використання SDN доведені на прикладі побудови корпоративних мереж на базі контролера APIC-ЕМ фірми Cisco.

SDN DEPLOYMENT IN ENTERPRISE NETWORKS BASED ON CISCO APIC-EM CONTROLLER

Pyavchyk M.O.

Scientific adviser: **Grygorenko O.G.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: max140699@gmail.com

The purpose and features of SDN technology are considered. The effectiveness and benefits of using SDNs are proved by the example of enterprise networks design based on Cisco APIC-EM controller.

ТЕХНОЛОГІЯ ПЕРЕДАЧІ ГОЛОСУ В МЕРЕЖІ LTE

Ветошко І.П.

Науковий керівник: **Носков В.І.**

Інститут телекомунікаційних систем,

КПІ ім. Ігоря Сікорського, Україна

E-mail: ivanvetoshko16@gmail.com

На сьогоднішній день перед операторами мобільного зв'язку постало завдання міграції голосового трафіку в мережі з комутацією пакетів. В ході роботи було розглянуто технологію передачі голосу в мережі LTE. Проаналізовано ефективність та переваги впровадження. Приведена концепція IMS, як опорна мережа для організації голосових сервісів.

VOICE OVER LTE TECHNOLOGY

Vetoshko I.P.

Scientific adviser: **Noskov V.I.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: ivanvetoshko16@gmail.com

Today mobile operators have been tasked with migrating voice traffic to a packet-switched network. LTE voice technology was considered in this work. The effectiveness and benefits of the implementation were analyzed. The concept of IMS as a support network for the organization of voice services is given.

MACHINE LEARNING USING TENSORFLOW

Tushych A.M.

Scientific adviser: **Storchak K.P.**

Educational and Scientific Institute of Information Technologies

State University of Telecommunications

E-mail: alinatushych@gmail.com

TensorFlow is an open load library for machine learning developed by Google. It has been applied solving problems of classification, clustering, regression and forecasting. TensorFlow, in neural network, attracts us by its simplicity, because it is based on the concept of computing graphs - constructing graphs of operations into which data and commands for computing are passed.

The basics of library work have been analyzed in the paper, the features of artificial neural network construction and a set of TensorFlow visualization tools have been studied.

МАШИННЕ НАВЧАННЯ З ВИКОРИСТАННЯМ TENSORFLOW

Тушич А.М.

Науковий керівник: **Сторчак К.П.**

Навчально-науковий інститут інформаційних технологій

Державний університет телекомунікацій

E-mail: alinatushych@gmail.com

TensorFlow – відкрита програмна бібліотека для машинного навчання, розроблена компанією Google. Знайшла застосування під час розв’язання задач класифікації, кластеризації, регресії та прогнозування. TensorFlow для розробки нейронних мереж приваблює своєю простотою, адже базується на концепції графів обчислень – побудові графів операцій, у які передаються дані та команди про виконання обчислень.

У роботі проаналізовано основи роботи бібліотеки, досліджено особливості побудови штучної нейронної мережі та набір інструментів візуалізації TensorFlow.

МАКЕТ АВТОМАТИЗОВАНОГО АНТЕННОГО ТРЕКЕРА ДЛЯ ПРИЙОМУ СИГНАЛІВ З МЕТЕОРОГІЧНИХ СУПУТНИКІВ

Мрига С.В.

Науковий керівник: **Коваль Д.В.**

Житомирський військовий інститут імені С.П. Корольова

E-mail: smartradio.koval@gmail.com

Сигнали метеосупутників NOAA та Метеор передаються у діапазонах 137 МГц, 1700 МГц та 8200 МГц. Приймання сигналів у діапазоні 137 МГц можливо здійснювати на неспрямовану антену. Однак, супутник Метеор-М №2, запущений у 2014 році, періодично стає причиною конфлікту із супутником NOAA-18, оскільки сигнали з вказаних космічних апаратів співпадають за частотою. Наслідком є практичне унеможливлення приймання сигналів з обох супутників у той час, коли вони обидва знаходяться у зоні огляду.

Розроблений антенний трекер дозволяє організувати процес слідкування за обраним супутником шляхом обертання спрямованої антени. Таким чином, здійснюється просторова селекція сигналів та роз'язується конфлікт супутників Метеор-М №2 та NOAA-18.

A MODEL OF AUTOMATED ANTENNA TRACKER FOR RECEIVING SIGNALS FROM WEATHER SATELLITES

Mryha S.V.

Scientific adviser: **Koval D.V.**

S.P. Koroliov Zhytomyr military institute

E-mail: kyiv12@bigmir.net

NOAA and Meteor weather satellites signals are transmitted in the 137 MHz, 1700 MHz and 8200 MHz bands. 137 MHz signals can be received on a non-directional antenna. However, the Meteor-M No. 2 satellite, launched in 2014 periodically causes conflict with the NOAA-18 satellite as the signals from these spacecraft coincide in frequency. The result is the practical inability to receive signals from both satellites while they are both in the viewing area.

An antenna tracker model developed allows to organize tracking the selected satellite by rotating the directional antenna. Thus, the spatial selection of signals is carried out and the conflict of Meteor-M No. 2 and NOAA-18 satellites is resolved.

LOCALIZATION IN VEHICLE NETWORKS USING RADIO FREQUENCY IDENTIFICATION TECHNOLOGY

M'Tumbe Abi Tresor

Scientific adviser: **Yeremenko O.S.**

Kharkiv National University of Radio Electronics, Ukraine

E-mail: mtumbeabitresor560@gmail.com

The incorporation of electronic systems of objects including sensor nodes, communication platforms and interactive objects in the domain of IoT are explored. The use of Radio Frequency Identification (RFID) in road transport includes speed monitoring automatically and access to data to get information, as well as vehicle detection in dense urban areas and in underground tunnels. The localization of vehicle using RFID in traffic that provides the position of the vehicle to present the identity and all information automatically has been investigated. The vehicle can obtain data from different positions with enabling RFID technologies. The multiple advantages are visible in these current fields where RFID technology is used.

ЛОКАЛІЗАЦІЯ В АВТОМОБІЛЬНИХ МЕРЕЖАХ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ РАДІОЧАСТОТНОЇ ІДЕНТИФІКАЦІЇ

М'Тумбе Абі Трезор

Науковий керівник: **Єременко О.С.**

Харківський національний університет радіоелектроніки, Україна

E-mail: mtumbeabitresor560@gmail.com

Досліджено інтеграцію електронних систем об'єктів, які включають сенсорні вузли, комунікаційні платформи та інтерактивні об'єкти в рамках IoT. Використання радіочастотної ідентифікації (Radio Frequency Identification, RFID) в автодорожньому транспорті включає автоматичний моніторинг швидкості та доступ до даних для отримання інформації, а також виявлення транспортних засобів у щільних міських районах і в підземних тунелях. Досліджено локалізацію транспортного засобу, що використовує RFID, у дорожньому русі, що автоматично надає його положення та всієї інформації. Транспортний засіб може отримувати дані з різних позицій за допомогою технологій RFID. Використання технології RFID має багато переваг.

SECURITY FRAMEWORK FOR IOT DEVICES

Egbe Godson Agbara

Scientific adviser: **Yeremenko O.S.**

Kharkiv National University of Radio Electronics, Ukraine

E-mail: egbedorian@gmail.com

Internet of Things (IoT) technology is the next technological leap that will introduce a significant improvement to people by connecting devices, people and networks together and no facet of the human environment. IoT devices are by nature highly connected hence it provides broad attack platform for hackers to exploit, consequently it needs a robust security model to support resource-constrained IoT devices and end to end security. The attack vectors and security requirements for IoT system and organizational approach towards security were investigated. The security architecture to provide security-enabled IoT services were explained, which proposed the framework divided into three parts: the application, network, and physical.

СИСТЕМА БЕЗПЕКИ ДЛЯ ІОТ ПРИСТРОЇВ

Егбе Годсон Агбара

Науковий керівник: **Єременко О.С.**

Харківський національний університет радіоелектроніки, Україна

E-mail: egbedorian@gmail.com

Технологія Інтернету речей (Internet of Things, IoT) – це наступний технологічний стрибок, який внесе значне вдосконалення для людей, з'єднавши пристрої, користувачів і мережі разом. Пристрої в мережі IoT за своєю природою мають високу зв'язність, тому вони забезпечують широку платформу для атак та використання хакерами, отже, їй потрібна надійна модель безпеки для підтримки обмежених ресурсами IoT-пристроїв і забезпечення захисту. Досліджено вектори атак та вимоги безпеки для системи IoT та організаційний підхід до безпеки. Була пояснена архітектура безпеки для забезпечення IoT-послуг, запропонована структура якої розділена на три частини: прикладну, мережну та фізичну.

