



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

**ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ
НДІ ТЕЛЕКОМУНІКАЦІЙ**

**П'ятнадцята міжнародна
науково-технічна конференція
" ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ"
і**

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

Присвячено Дню науки та Всесвітньому Дню телекомунікацій

12–16 квітня 2021 року

Матеріали конференції

м. Київ



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

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

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

and

**Thirteenth 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 12-16, 2021

Conference proceedings

Kyiv

XV Міжнародна науково-технічна конференція "Перспективи телекомунікацій" ПТ-2021: Збірник матеріалів конференції. К.: КПІ ім. Ігоря Сікорського, 2021. – с.408.

XV International Scientific Conference "**Modern Challenges in Telecommunications**" MCT-2021. Conference proceedings. Kyiv. Igor Sikorsky Kyiv Polytechnic Institute, 2021 – p. 408.

XIII Міжнародна науково-технічна конференція студентів та аспірантів «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем» ПРІТС 2021: Збірник тез конференції. К.: КПІ ім. Ігоря Сікорського, 2021.

Збірник містить матеріали пленарних і секційних доповідей, представлених на П'ятнадцятій міжнародній науково-технічній конференції "Перспективи телекомунікацій" (ПТ 2021) та Тринадцятій міжнародній науково-технічній конференції студентів та аспірантів «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем» (ПРІТС 2021), дати проведення 12–16 квітня 2021 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. – директор Інституту телекомунікаційних систем Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", академік НАНУ, д.т.н., професор;

БАРАНОВ О.А. – керівник Науково-дослідного центру цифрових трансформацій і права Науково-дослідного інституту інформатики і права при Національній академії правових наук (НДІП НАПрН) 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;
КОТ Т.М. - Dr.-Eng., Solutions Architect, NVision Czech Republic, Прага, Чехія;
ЛЕМЕСЬКО 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;
МІНОЧКІН Д.А. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
МОШИНСЬКА А.В. - д.т.н., с.н.с., 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 «МАН України», Київ;
ТЕНШИ Хара - Dr.-Eng. Technical University of Dresden, Дрезден, Німеччина;
ТОЛЮПА С.В. – д.т.н., проф., НУ ім. Т. Шевченка, 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;
ШПЛЬНЕР 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 І 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:

Конференцію було проведено дистанційно за допомогою on-line сервісів для відеоконференцій та вебінарів ZOOM та Meet.

ЗМІСТ

Пленарні доповіді

Доповідачі:

С.О. Кравчук, М.Ю. Ільченко

ЩОДО ПРОВЕДЕННЯ ЛЕКЦІЙНИХ ЗАНЯТЬ В ДИСТАНЦІЙНОМУ РЕЖИМІ.....19

В.А. Романюк, О. І. Лисенко, А.В. Романюк, А.Г. Гримуд

МЕТОД БЕЗПОСЕРЕДНЬОГО ЗБОРУ ДАНИХ З ВУЗЛІВ
БЕЗПРОВОДОВОЇ СЕНСОРНОЇ МЕРЕЖІ ТЕЛЕКОМУНІКАЦІЙНИМИ
АЕРОПЛАТФОРМАМИ.. 23

L.S. Globa, R.L. Novograduska, B.O. Zadoienko and Yu Junfeng

ONTOLOGY-BASED APPROACH TO SCIENTIFIC
INSTITUTIONS INFORMATION REPRESENTATION. 26

В.І.Новіков

МЕТОД ПІДВИЩЕННЯ ПРОПУСКНОЇ ЗДАТНОСТІ МОБІЛЬНИХ
БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ НА ОСНОВІ
ВИКОРИСТАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ АЕРОПЛАТФОРМ 30

К. Лісовський, Н. Кириндась, М. Ільченко, О. Живков,

Є. Куліков, Д. Субботський

ПЕРСПЕКТИВИ РОЗВИТКУ ПРОЕКТУ СУПУТНИКОВОГО ЗВ'ЯЗКУ
STARLINK В УКРАЇНІ 34

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:

Вістунов В.Д., Гаттуров В.К.

АНАЛІЗ ПОБУДОВИ МЕРЕЖ ДОСТУПУ НА ОСНОВІ СУЧАСНИХ
ШИРОКОСМУГОВИХ ТЕХНОЛОГІЙ.....38

Мєщерінов М.В., Гаттуров В. К.

ДОСЛІДЖЕННЯ ПРОДУКТИВНОСТІ МЕРЕЖІ NGN НА БАЗІ IMS
ПРИ ПЕРЕДАЧІ ТРАФІКУ МЕРЕЖІ ЗКС №7 ЗА УМОВИ ВТРАТИ
ПАКЕТІВ ПРИ ВИКОРИСТАННЯМ ПРОТОКЛІВ UDP ТА SCTP 41

Григоренко О.Г., Полікарпова Ю.Г. ВИКОРИСТАННЯ АУТЕНТИФІКАЦІЇ В МЕРЕЖІ ЯК СПОСОБУ ВИКОНАННЯ БЕЗПЕЧНИХ ХМАРНИХ ОБЧИСЛЕНЬ	44
Козак А.Ю., Могилевич Д.І. АНАЛІЗ МЕТОДІВ ОЦІНКИ ПОКАЗНИКІВ ЯКОСТІ ОБСЛУГОВУВАННЯ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ	47
Уривський Л.О., Мартинова К.Г. ДОСЛІДЖЕННЯ ПОКАЗНИКІВ ЧУТЛИВОСТІ ХАРАКТЕРИСТИК СМО З ПРІОРИТЕТАМИ ДО ЗМІН СТРУКТУРИ ОБСЛУГОВУВАННЯ ..	50
Уривський Л.О., Шмігель Б.О. ВИЗНАЧЕННЯ ЗАВАДОСТІЙКОСТІ СКК В УМОВАХ НИЗЬКОЇ ЕНЕРГЕТИКИ	53
Вакуленко О.В., Кирилова В.Д. ПОБУДОВА КОМП'ЮТЕРНИХ КЛАСТЕРІВ ДЛЯ МОДЕЛЮВАННЯ НАДСКЛАДНИХ ПРОЦЕСІВ У ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ НА БАЗІ ОПЕРАЦІЙНОЇ СИСТЕМИ LINUX	56
Вакуленко О.В., Єрохін В.Ф. УДОСКОНАЛЕНА МЕТОДИКА СИНТЕЗУ АЛГОРИТМІВ ВИЯВЛЕННЯ-РОЗДІЛЕННЯ ВЗАЄМНО НЕОРТОГОНАЛЬНИХ СИГНАЛІВ ПРИ ПАКЕТНОМУ РЕЖИМІ ПЕРЕДАЧІ	59
Уривський Л. О., Корнієнко А. А. МЕТОДИКА ВИЗНАЧЕННЯ ПАРАМЕТРУ ШВИДКОСТІ КОДУВАННЯ ЗА АЛГОРИТМОМ УПРАВЛІННЯ СИТУАЦІЄЮ В КАНАЛІ ЗВ'ЯЗКУ ПРИ НЕЗМІННОСТІ ПРОДУКТИВНОСТІ ДЖЕРЕЛА ПОВІДОМЛЕНЬ	62
Максимов В.В., Храповицький І.А. ДОСЛІДЖЕННЯ НОВИХ КОМПОЗИТНИХ КОДІВ БАРКЕРА	66
Уривський Л.О., Солянікова В.Ю. ВПЛИВ БАГАТОПРОМЕНЕВОСТІ НА КАНАЛ МОБІЛЬНОГО ЗВ'ЯЗКУ В ГІГАГЕРЦОВОМУ ДІАПАЗОНІ ХВИЛЬ	69

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:

Сливка А.Р., Авдєєнко Г.Л. АПАРАТНО-ПРОГРАМНИЙ КОМПЛЕКС НА БАЗІ МОДУЛЯТОРІВ ДЕКТЕС ДЛЯ ФОРМУВАННЯ ТА ДОСЛІДЖЕННЯ СИГНАЛІВ ЦИФРОВОГО ТЕЛЕВІЗІЙНОГО МОВЛЕННЯ	73

Пащенко А.І., Трубін О.О. МОДЕЛЮВАННЯ 2-РЕЗОНАТОРНОГО ADD-DROP ФІЛЬТРА НА МІКРОКІЛЬЦЕВИХ РЕЗОНАТОРАХ.....	76
Zhivkov A., Akopian P., Galickiy I., Krylach O., Kopaniev M., Kamarali R. MICROWAVE FILTERS WITH VARIABLE PARAMETERS BASED ON CELLS OF METAMATERIALS	79
Trubarov I.V. DESIGN AND OPTIMIZATION OF TWO-RESONATOR INSET-FED PRINTED PATCH ANTENNA FOR 2.4 GHZ FREQUENCY BAND.....	83
Trubarov I.V. DESIGN AND OPTIMIZATION OF COAXIAL-FED RECTANGULAR TWO-RESONATOR PATCH ANTENNA FOR 2.4 GHZ FREQUENCY BAND.....	86
Trubin A. A. COUPLING COEFFICIENTS OF ROTATING RECTANGULARE DIELECTRIC RESONATORS IN CUT-OFF RECTANGULARE WAVEGUIDE	89
Trubin A. A. SCATTERING OF PLANE WAVES ON CUBIC SHAPE DIELECTRIC RESONATORS.....	92

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:

Корнієнко Н.І., Романов А.О. ПОБУДОВА SDN-КОНТРОЛЕРА НА БАЗІ ВІДКРИТОЇ МЕРЕЖЕВОЇ ОПЕРАЦІЙНОЇ СИСТЕМИ ONOS	95
Романов О.І., Марінов А.І., Сколець С.С. ДОСЛІДЖЕННЯ МЕРЕЖ SDN З ВИКОРИСТАННЯМ ПЛАТФОРМИ MININET.....	98
Маньківський В.Б., Педько А.Д. АНАЛІЗ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ TSP В МЕРЕЖАХ LTE ..	102
Нестеренко М.М., Топорков М.А. МОВА ПРОГРАМУВАННЯ P4 МЕРЕЖЕВИХ ПРИСТРОЇВ SDN	106

Романов О.І., Марінов А.І., Сколець С.С. ДОСЛІДЖЕННЯ ПОКАЗНИКІВ ФУНКЦІОНУВАННЯ МЕРЕЖІ SDN З ВИКОРИСТАННЯМ MININET I FLOODLIGHT CONTROLLER.....	109
Тріска Н.Р. ПИТАННЯ ВПРОВАДЖЕННЯ СТАНДАРТУ 5G НА БАЗІ ІСНУЮЧОЇ ІНФРАСТРУКТУРИ МЕРЕЖІ	113
Атаманчук М.В., Сайченко І.О. ПІДВИЩЕННЯ НАДІЙНОСТІ ФУНКЦІОНУВАННЯ МЕРЕЖ SDN МЕТОДОМ РЕЗЕРВУВАННЯ КОНТРОЛЕРІВ	116
Романов О. І., Шаповалов Р. С. ВИКОРИСТАННЯ ТЕХНОЛОГІЇ SDN ПРИ ПОБУДОВІ КАМПУСНОЇ МЕРЕЖІ LI-FI	120
Кочура М.Ю., Романов М.О. ПОБУДОВА SDN МЕРЕЖІ ШИРОКОСМУГОВОГО ДОСТУПУ НА БАЗІ ПЛАТФОРМИ RESIDENTIAL CORD.....	123
Бурлака Г.Ю. MININET: СИМУЛЯТОР ДЛЯ СТВОРЕННЯ І ПРОЕКТУВАННЯ ПРОТОТИПІВ МЕРЕЖ SDN	126
Мікляєв Г.О. ЗАСАДИ ПРОЕКТУВАННЯ ОФІСНОЇ МЕРЕЖІ НА БАЗІ ТЕХНОЛОГІЇ Li-Fi.....	129
Полуденний О. М., Цуканов О. Ф. ОЦІНКА БЕЗПЕКИ ТА АНАЛІЗ ВРАЗЛИВОСТІ IP MULTIMEDIA SUBSYSTEM (IMS).....	132
Верес Л.А. МЕТОД РОЗРАХУНКУ НАДІЙНОСТІ РІВНЯ УПРАВЛІННЯ АРХІТЕКТУРИ IMS ПРИ КОВЗНОМУ РЕЗЕРВУВАННІ.....	136

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:

Новіцька А.О., Капштик С.В., Наритник Т.М. ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ В СУПУТНИКОВІЙ СИСТЕМІ ІНТЕРНЕТУ РЕЧЕЙ НА БАЗІ ПРОТОКОЛУ LoRaWAN	139
Правило В. В., Хижняк С. П. ПРОБЛЕМИ КІБЕРБЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ	143

Денисенко Н. І., Авдєєнко Г. Л. ОГЛЯД ТА АНАЛІЗ ІСНУЮЧИХ АЛГОРИТМІВ РАДІОПЕЛЕНГАЦІЇ ДЖЕРЕЛ ВИПРОМІНЮВАННЯ ДЛЯ РАДІОТЕХНІЧНИХ СИСТЕМ	146
Скрябін С.А., Носков В.І. КРИТЕРІЇ ОЦІНКИ ЕФЕКТИВНОСТІ РАДІОКАНАЛІВ МЕРЕЖ LTE ...	149
Міхненко Я.О., Курдеча В.В. СУЧАСНА ПРОБЛЕМАТИКА ІНТЕРНЕТУ РЕЧЕЙ	152
Правило В.В., Бірчин М.А. АРХІТЕКТУРА МЕС В МОБІЛЬНИХ МЕРЕЖАХ 4G.....	155
Василенко С.В. АНАЛІЗ ЗАВАДОЗАХИЩЕНОСТІ ПРОЦЕСУ ВХОДЖЕННЯ В СИНХРОНІЗМ РАДІОЛІНІЇ УПРАВЛІННЯ БПЛА З ППРЧ.....	158
Кормульов О.С. ВДОСКОНАЛЕНА МОДЕЛЬ БЕЗПЕКИ 5G.....	161
Правило В. В., Хижняк О. П. ТЕХНОЛОГІЯ 5G І ЇЇ ВПЛИВ НА ІНТЕРНЕТ РЕЧЕЙ	164
Ветошко І.П., Носков В.І. ПАРАМЕТРИ ОЦІНКИ ЯКОСТІ ГОЛОСОВОГО ТРАФІКУ В МЕРЕЖАХ LTE	167
Ільченко М.Ю., Кайденко М.М. ОСОБЛИВОСТІ РАДІОЧАСТОТНОЇ ФІЛЬТРАЦІЇ В SDR СИСТЕМАХ	170
Кравчук С.О., Кравчук І.М. АНАЛІЗ МОДЕЛЕЙ ВТРАТ НА ПОШИРЕННЯ ДЛЯ РАДІОЛІНІЙ ЗЕМЛЯ-ПОВІТРЯ.....	173
Кравчук С.О., Рисцова К.І. АПРОКСИМАЦІЯ ДІАГРАМИ СПРЯМОВАНOSTІ АНТЕНИ БАЗОВОЇ СТАНЦІЇ	176
Гетьман О.В., Кайденко М.М., Роскошний Д.В. ЗАГРОЗИ БЕЗПЕЦІ ТА ПРОБЛЕМИ ВРАЗЛИВОСТІ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ	180
Кайденко М.М., Роскошний Д.В. ОСОБЛИВОСТІ ЗАСТОСУВАННЯ SYSTEM-ON-CHIP INTEL ТА XILINX ПРИ РОЗРОБЦІ SDR СИСТЕМ	183
Афанасьєва Л.О., Кравчук С.О. ДОСЛІДЖЕННЯ ВИКОРИСТАННЯ АПАРАТНИХ ТЕХНОЛОГІЙ 60 ГГЦ СТАНДАРТУ IEEE 802.11AD ДЛЯ ЗАСТОСУВАННЯ В МІСЬКІЙ ЗАБУДОВІ.....	186

Урніш В. С., Кравчук С. О. КООПЕРАТИВНА РЕТРАНСЛЯЦІЯ НА ОСНОВІ АДАПТИВНОГО ДЕКОДУВАННЯ	189
Остапов О.А., Шевченко І.І., Чуб М.М. ОСОБЛИВОСТІ ТЕСТУВАННЯ СИСТЕМ З МІКРОСЕРВІСНОЮ АРХІТЕКТУРОЮ	192
Нагорна М.М., Кравчук С.О. ПРОТОКОЛ ЗАПОБІГАННЯ КОЛІЗІЙ В МЕРЕЖІ ІоТ З ВИКОРИСТАННЯМ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ.....	195
Кайдено М.М. ЗАХИЩЕНА ВІД ВПЛИВУ НАВМИСНИХ ЗАВАД СИСТЕМА ЗВ'ЯЗКУ МАЛОГАБАРИТНИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ	199
Токаренко М.Я., Кравчук С. О. МЕТОДИ І ТЕХНОЛОГІЇ ПОЗИЦІОНУВАННЯ ДЛЯ ВІРТУАЛЬНОЇ РЕАЛЬНОСТІ.....	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:

Тимофєєв Є.М., Созонник Г.Д. АНАЛІЗ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СЕРВІСІВ MPLS VPN.....	204
Корман Н.А., Могилевич Д.І. АНАЛІЗ ВИКОРИСТАННЯ ПРОТОКОЛІВ IPSEC ТА SSL В КОРПОРАТИВНИХ МЕРЕЖАХ.....	207
Глоба Л.С., Савчук З.Р. QOS АНАЛІЗ МЕРЕЖ ПЕРЕДАЧІ ДАНИХ НА ОСНОВІ НЕЧІТКОЇ БАЗИ ЗНАНЬ	211
Копа Р.В., Штогріна О. С. ПІДХІД ДО ДОСЛІДЖЕННЯ ПСИХОФІЗІОЛОГІЧНОГО СТАНУ ЛЮДИНИ НА ОСНОВІ МЕТОДІВ МАШИННОГО НАВЧАННЯ.....	215
Бугаєнко Ю.М., Ляшенко А.В. АРХІТЕКТУРНЕ РІШЕННЯ ЩОДО СИСТЕМИ АНАЛІЗУ ДАНИХ ОБЧИСЛЮВАЛЬНИХ ПРОЦЕСІВ.....	218

Берлоус В.О., Штогріна О.С. ПРОБЛЕМНІ ПИТАННЯ ПРИ ВИКОРИСТАННІ КОНЦЕПЦІЇ ЛІТ В ПРОМИСЛОВОМУ ВИРОБНИЦТВІ І СПОСОБИ ЇХ ВИРІШЕННЯ	222
Ладичук О.К., Попова М.А. ЗАСТОСУВАННЯ ОНТОЛОГІЙ В ТЕЛЕКОМУНІКАЦІЯХ	225
Зайченко Ю.П., Васильєв В.І., Вішталъ Д.М., Любашенко Н.Д. АЛГОРИТМИ УКРУПНЕННЯ СТАНІВ МЕРЕЖІ ПЕРЕДАЧІ ДАНИХ В ЗАДАЧАХ ОЦІНКИ МЕРЕЖЕВИХ ХАРАКТЕРИСТИК	228
Вакуленко О.В., Дорошенко А.С., Луцький А.О. ПРОЕКТУВАННЯ МУЛЬТИСЕРВІСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ВІДОМЧОГО ПРИЗНАЧЕННЯ НА ОСНОВІ БАГАТОКРИТЕРІАЛЬНОГО ПІДХОДУ	232
Гребініченко М.В. ОЧИЩЕННЯ ДАНИХ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ОБРОБКИ ДАНИХ В МЕРЕЖАХ ІОТ	235
Смаглюк В.О., Алексєєв М.О. ВИКОРИСТАННЯ ОБЧИСЛЮВАЛЬНИХ ПОТУЖНОСТЕЙ МОБІЛЬНИХ ПРИСТРОЇВ ТА ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ У КОРПОРАТИВНІЙ МЕРЕЖІ.....	238
Бугаєнко Ю.М., Врачинська А. О. МОДИФІКОВАНИЙ АЛГОРИТМ ПОПЕРЕДНЬОЇ ОБРОБКИ НЕЧІТКИХ ЛОГІЧНИХ ПРАВИЛ	241
Ушаков С.М., Курдеча В.В. МЕТОД ОБРОБКИ ІНФОРМАЦІЇ НА ОСНОВІ НЕЙРОМЕРЕЖ ДЛЯ МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ	244
Гіззатуллін Д. Д., Курдеча В.В. МЕТОД ВІЯВЛЕННЯ ВТОРГНЕНЬ В МЕРЕЖІ ІОТ	247
Петров О.С., Курдеча В.В. АНАЛІЗ МЕТОДІВ ЗАХИСТУ ДАНИХ В МЕРЕЖІ INTERNET OF THINGS.....	250
Сегеда С.А., Алексєєв М.О. ПІДХІД ДО ОРКЕСТРУВАННЯ ВЕБ-СЕРВІСІВ У КЛАСТЕРІ, ЩО ВИКОРИСТОВУЄ РЕСУРСИ ПРИСТРОЇВ У КОРПОРАТИВНІЙ МЕРЕЖІ.....	253

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:

Новіков В.І., Лисенко О.І., Алексєєва І.В.

УДОСКОНАЛЕННЯ МАТЕМАТИЧНОЇ МОДЕЛІ ОЦІНКИ
ЗВ'ЯЗНОСТІ ВУЗЛІВ МОБІЛЬНОЇ БЕЗПРОВОДОВОЇ СЕНСОРНОЇ
МЕРЕЖІ ІЗ ТЕЛЕКОМУНІКАЦІЙНИМИ АЕРОПЛАТФОРМАМИ 257

Явіся В.С., Лисенко О.І.

МЕТОД РЕАЛІЗАЦІЇ КОНЦЕПЦІЇ «CLEAR SPACE» 261

Явіся В.С., Лисенко О.І.

СТРУКТУРА РОЗПОДІЛЕНОГО ТЕЛЕКОМУНІКАЦІЙНОГО
СУПУТНИКА 264

Явіся В.С., Лисенко О.І.

СИСТЕМИ ЖИТТЕЗАБЕЗПЕЧЕННЯ ТЕЛЕКОМУНІКАЦІЙНОГО
НАНОСУПУТНИКА..... 267

Неуймін О. С., Соколов К.А., Маленчик Т.В.

АНАЛІЗ МЕТОДУ ВИЯВЛЕННЯ ТОЧКОВИХ ЦІЛЕЙ НА ОСНОВІ
МОДЕЛІ ІНФРАЧЕРВОНОГО ПАТЧ-ЗОБРАЖЕННЯ 271

Валуйський С.В., Собко Т.А.

АНАЛІЗ ЗАГРОЗ ТА МЕТОДІВ ЗАХИСТУ МЕРЕЖ ВІД XSS АТАК
ТА SQL ІН'ЄКЦІЙ 274

Лисенко О.І., Роспутній В.В.

АНАЛІЗ СПОСОБІВ ПОБУДОВИ ТА ФУНКЦІОНУВАННЯ
СЕНСОРНИХ РАДІОМЕРЕЖ ІЗ ВИКОРИСТАННЯМ SDN..... 277

Турчин Я.В., Валуйський С.В.

МЕТОД ПІДВИЩЕННЯ ЗВ'ЯЗНОСТІ МЕРЕЖ MANET ІЗ
ВИКОРИСТАННЯМ БПЛА 280

Гордійко Н.О., Томашевська Т.В.

МЕТОД ПРОЕКТУВАННЯ РОЗМІЩЕННЯ ДАТЧИКІВ 283

Якорнов Є.А., Цуканов О.Ф. МОДЕЛЮВАННЯ ПАРАМЕТРІВ РУХУ МАНЕВРУЮЧИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ НА ОСНОВІ СТІЙКОГО АЛГОРИТМУ ДИНАМІЧНОЇ ФІЛЬТРАЦІЇ.....	286
Цуканов О.Ф., Якорнов Є.А. РОБАСТНОСТНИЙ ПІДХІД ДО ЗАДАЧІ ПІДВИЩЕННЯ ТОЧНОСТІ ВИЗНАЧЕННЯ КООРДИНАТ ЕЛЕМЕНТІВ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ.....	289
Жук С.Я., Герасименко А.О., Соколов К.А. АНАЛІЗ ТОЧНОСНИХ ХАРАКТЕРИСТИК КОРЕЛЯЦІЙНО- ЕКСТРЕМАЛЬНОГО АЛГОРИТМУ СТЕЖЕННЯ ЗА МАЛОРОЗМІРНИМ БПЛА З ВИКОРИСТАННЯМ ФІЛЬТРУ КАЛМАНА	292
Лисенко О.І., Самберг А., Чумаченко С.М., Новіков В.І. АНАЛІЗ ФУНКЦІОНАЛЬНОЇ ЖИВУЧОСТІ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ.....	295
Новіков В.І., Дворська С.В., Дакова Л.В. ЗАСТОСУВАННЯ МУЛЬТИМЕТРИЧНИХ ПРОТОКОЛІВ ТА МІЖШАРОВОГО ПІДХОДУ ДЛЯ ПІДВИЩЕННЯ ЕНЕРГОЕФЕКТИВНОГО ФУНКЦІОНУВАННЯ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ.....	298
Товкач І.О., Васильєв В.М., Чмельов В.О., Путієнко О.М. АНАЛІЗ ВПЛИВУ КОНФІГУРАЦІЇ СЕНСОРНОЇ МЕРЕЖІ НА ТОЧНІСТЬ ВИЗНАЧЕННЯ МІСЦЕПОЛОЖЕННЯ ДЖЕРЕЛА РАДІОВИПРОМІНЮВАННЯ НА ОСНОВІ АОА- ВИМІРЮВАНЬ	301
Лапа Є.О., Лисенко О.І., Савченко А.О. АНАЛІЗ ТЕХНОЛОГІЙ ТА ПАРАМЕТРІВ ФУНКЦІОНУВАННЯ ІОТ МЕРЕЖ	304
Штойко О.О., Лисенко О. І. РОЗВИТОК МЕТОДІВ МАРШРУТИЗАЦІЇ В МОБІЛЬНИХ СЕНСОРНИХ МЕРЕЖАХ.....	307
Сергійчук Д. М., Лисенко О. І. РОЗВИТОК АЛГОРИТМІВ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ МІМО У МОБІЛЬНИХ СЕНСОРНИХ МЕРЕЖАХ.....	310

Нідченко І. А., Лисенко О. І. КОМУНІКАЦІЯ З СЕРВІСНИМ РОБОТОМ ПРИ УПРАВЛІННІ МІНІТЕПЛИЦЕЮ	313
Руренко О.Г. МОДЕЛЬНІ ІГРОВІ ЗАДАЧІ ДЛЯ СИСТЕМ ЛІНІЙНИХ РІВНЯНЬ З ДРОБОВИМИ ПОХІДНИМИ КАПУТТО І РІМАНА-ЛІУВІЛЯ	316
Валуйський С.В., Єфименко О.С. АНАЛІЗ ЗАСТОСУВАННЯ МЕТОДІВ МАРШРУТИЗАЦІЇ В AD NOS МЕРЕЖАХ ІЗ БПЛА	319
Кучеренко А.А. ПІДХОДИ ДО ЕНЕРГОЗБЕРЕЖЕННЯ В БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ.....	322
Осинський А.К., Лисенко О. І. РОЗВИТОК МЕТОДУ МАРШРУТИЗАЦІЇ В БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ НА ОСНОВІ ЗАСТОСУВАННЯ АЛГОРИТМУ ВИБОРУ ГОЛОВНИХ КЛАСТЕРНИХ ВУЗЛІВ	325
Синявіна Є.П. СИНХРОНІЗАЦІЯ ЧАСУ В БЕЗПРОВІДНИХ СЕНСОРНИХ МЕРЕЖАХ	328

Секція 7. Системна й програмна інженерія інфокомунікацій

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

Доповідачі:

Гребенніков В.О. ІНФОРМАЦІЙНА ФІЛОСОФІЯ ТЕЛЕКОМУНІКАЦІЙ	331
Нарушкевич О.М., Жабчик А.І., Капштик С.В., Наритник Т.М. ГЕОСТАЦІОНАРНА СУПУТУНІКОВА ІНФРАСТРУКТУРА ІНТЕРНЕТУ РЕЧЕЙ.....	336
Дуля О.О., Міночкін Д.А. МЕТОДИ АУТЕНТИФІКАЦІЇ НА ОСНОВІ ПУБЛІЧНОГО КЛЮЧА В СИСТЕМІ ІНТЕРНЕТУ РЕЧЕЙ.....	340
Вигівський М.С., Денисенко М.С., Капштик С.В., Наритник Т.М. ВИКОРИСТАННЯ ЦИФРОВИХ АНТЕННИХ РЕШІТОК ДЛЯ ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ ПРИЙОМУ СИГНАЛІВ НАВІГАЦІЙНОЇ СИСТЕМИ GPS	343

Нсер А.М., Міночкін Д.А. ОГЛЯД СУПУТНИКОВОГО ІНТЕРНЕТУ STARLINK	347
Нікішин В. Ю., Міночкін Д.А. АНАЛІЗ ТЕХНІЧНИХ РІШЕНЬ ДЛЯ ПОБУДОВИ МЕРЕЖІ ІОТ НА ПІДПРИЄМСТВІ	350
Міночкін Д.А., Рибак О.О. ДОСЛІДЖЕННЯ СХЕМИ ADAPTIVE DATA RATE В ПРОТОКОЛІ ПЕРЕДАЧІ ДАНИХ LORAWAN	353
Тарновський А.М., Коляда К.В. СИСТЕМА ВІДДАЛЕНОГО КЕРУВАННЯ ДОСТУПОМ.....	356
Піхота К.В., Горицький В.М. СЕРТИФІКАЦІЯ КІБЕРБЕЗПЕКИ ІОТ: СИСТЕМА ТА СХЕМИ ОЦІНКИ ВІДПОВІДНОСТІ	359
Кочева Н.В., Горицький В.М. ОЦІНКА ВІДПОВІДНОСТІ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ: АКРЕДИТАЦІЯ ОРГАНІВ З ОЦІНКИ ВІДПОВІДНОСТІ.....	363

SEMINAR Modern information and telecommunication trends

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

Доповідачі:

Moshynska A.V., Sozonnik G.D., Maltsev A.G. RESEARCH OF ALGORITHMS OF SERVICE OF LOADINGS IN FOG – NETWORKS	367
Loboda R., Osypchuk S. IOT-SYSTEM DEVELOPMENT FOR ENERGY METERS DATA TRANSFER AND PROCESSING	370
Piavchyk M., Budishevskyi O., Osypchuk S. FOG-NETWORK WITH SMART CONTROL SYSTEM MODEL DEVELOPMENT.....	373
Bidukha D.O., Pravylo V.V. TRENDS AND FUTURE OF CLOUD TECHNOLOGIUES IN GAMING INDUSCTRY	376
Peleshok Y.V., Honenko S.V., Horlichenko S.O. THE COHERENT DEMODULATION PROCEDURE OF MUTUALLY NON-ORTHOGONAL DIGITAL SIGNALS	379

**Тринадцята 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:

Хижняк О. П. кер. Правило В. В.

АНАЛІЗ РОЗВИТКУ МОБІЛЬНИХ МЕРЕЖ П'ЯТОГО ПОКОЛІННЯ
В УКРАЇНІ.....384

Хижняк С. П. кер. Правило В. В.

АНАЛІЗ ВРАЗЛИВОСТЕЙ І НЕДОЛІКІВ КІБЕРБЕЗПЕКИ В МЕРЕЖІ
ІНТЕРНЕТУ РЕЧЕЙ.....385

Нескородов В.В. кер. Осипчук С.О

АНАЛІЗ ТЕЛЕКОМУНІКАЦІЙНИХ FOG-ІНФРАСТРУКТУР ДЛЯ
ОБСЛУГОВУВАННЯ ТРАФІКУ ІОТ 386

Тєльчарова Д. О. кер. Носков В. І.

ЕВОЛЮЦІЯ МЕРЕЖ GPON ТА GE-PON 387

Волох М.А. кер. Міночкін Д.А.

АНАЛІЗ СУЧАСНИХ СТАНДАРТІВ І ПЛАТФОРМ ДЛЯ
ПОБУДОВИ ІОТ СИСТЕМ.....388

Паршин А.Ю., кер. Носков В.І.

ТРАНСПОРТНІ МЕРЕЖІ НА ОСНОВІ ТЕХНОЛОГІЇ NG SDN 389

Криклива А.В. кер. Уривський Л.О.

АНАЛІЗ ВПЛИВУ ВЛАСТИВОСТІ САМОПОДІБНОСТІ ТРАФІКУ
НА ЯКІСТЬ ОБСЛУГОВУВАННЯ 390

Бубка Б.А. кер. Лисенко О.І.

РОЗВИТОК АЛГОРИТМІВ ПІДВИЩЕННЯ ПРОПУСКНОЇ
ЗДАТНОСТІ В МОБІЛЬНИХ СЕНСОРНИХ МЕРЕЖАХ.....391

Березовський І. М. кер. Носков В.І.

ТЕХНІЧНІ ПРИНЦИПИ ПЕРЕДАЧІ СИГНАЛІВ В МЕРЕЖАХ LTE.....392

Маслак М.О. кер. Носков В.І.

ТЕХНІЧНІ ПРИНЦИПИ ТРАНСПОРТНИХ МЕРЕЖ MPLS TP 393

Корман Н.А. кер. Могилевич Д.І.

ДОСЛІДЖЕННЯ ВИКОРИСТАННЯ ПРОТОКОЛІВ IPSEC ТА SSL В
КОРПОРАТИВНІЙ МЕРЕЖІ 394

Бовсуновський Д.Р. кер. Носков В.І. ТЕХНІЧНІ ПРИНЦИПИ ПОБУДОВИ ОПТИЧНИХ ТРАНСПОРТНИХ МЕРЕЖ	395
Москалюк С.О., кер. Руренко О.Г. ПРОЕКТУВАННЯ ІЄРАРХІЧНИХ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ ДЛЯ МОНІТОРИНГУ ТРУБОПРОВОДІВ.....	396
Гіззатуллін Д. Д. кер. Курдеча В.В. АНАЛІЗ ВРАЗЛИВОСТЕЙ МЕРЕЖІ ІОТ	397
Карлін П.Ю., кер. Курдеча В.В. МОДИФІКОВАНИЙ МЕТОД ВЗАЄМОДІЇ ВУЗЛІВ МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ.....	398
Ушаков С. М. кер. Курдеча В. В. АНАЛІЗ КОДУВАННЯ ДАНИХ В МЕРЕЖІ ІНЕТРНЕТУ РЕЧЕЙ	399
Березнюк А. В., Лазебний С.Г. кер. Макаренко А.О. УДОСКОНАЛЕНА АРХІТЕКТУРА ІОТ, ЗАСНОВАНА НА ТЕХНОЛОГІЯХ П'ЯТОГО ПОКОЛІННЯ	400
Петров О.С. кер. Курдеча В.В. ПРОБЛЕМИ ЗАХИСТУ ДАНИХ В МЕРЕЖІ INTERNET OF THINGS ...	401
Тимофєєв Є.М. кер. Созонник Г.Д. ОРГАНІЗАЦІЯ ПРОТИДІЇ ЗАГРОЗАМ ПОРУШЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	402
Персіков М.А., Лемешко В.О. кер. Єременко О.С. ОСОБЛИВОСТІ ВИКОРИСТАННЯ ЗАСОБІВ ШТУЧНОГО ІНТЕЛЕКТУ В ТЕХНОЛОГІЇ SECURE SD-WAN.....	403
Папушой О.К., кер. Могилевич Д.І. УДОСКОНАЛЕНА МЕТОДИКА ОЦІНКИ СТРУКТУРНОЇ НАДІЙНОСТІ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ ЗВ'ЯЗКУ	404
Круглова А.О., Журавльова А.С. кер. Лемешко О.В. ПОТОКОВА МОДЕЛЬ БАЛАНСУВАННЯ НАВАНТАЖЕННЯ В ІНФОКОМУНІКАЦІЙНІЙ МЕРЕЖІ	405
Бузян С.О. кер. Григоренко О.Г. РЕАЛІЗАЦІЯ МЕРЕЖІ І ДІЯЛЬНОСТІ СУЧАСНОЇ КОМПАНІЇ НА ОСНОВІ ПРОДУКТІВ MICROSOFT	406
Биков П.І. кер. Кононова І.В. АНАЛІЗ ВИКОРИСТАННЯ СУПУТНИКІВ НИЗЬКОЇ НАВКОЛОЗЕМНОЇ ОРБИТИ ДЛЯ ВИРІШЕННІ ЗАДАЧ ВСЕСВІТНЬОЇ МЕРЕЖЕВОЇ ВЗАЄМОДІЇ	407
Цимбал Г.О. кер. Григоренко О.Г. ПОБУДОВА ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ НА ОСНОВІ ТЕХНОЛОГІЇ MPLS	408

Пленарні доповіді

УДК 621.396.1

ЩОДО ПРОВЕДЕННЯ ЛЕКЦІЙНИХ ЗАНЯТЬ В ДИСТАНЦІЙНОМУ РЕЖИМІ

Ільченко М.Ю., Кравчук С.О.

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

ON LEARNING LECTURES IN THE REMOTE MODE

In this paper, the authors propose to answer two important methodological questions. What is the difference between the procedure for conducting a lecture in a distance mode from the usual traditional mode of conducting a lecture in the classroom? Need a modification of the traditional remote lecturing procedure to make it more effective?

Тема підвищення ефективності проведення занять (освітнього процесу) зі студентами завжди є актуальною для науково-викладацького персоналу будь-якого вищого навчального закладу [1-3]. Тим більше це актуально, коли доводиться проводити освітній процес в незвичних (нетрадиційних) умовах несприятливої епідеміологічної ситуації, пов'язаної з поширенням коронавірусної хвороби (COVID-19) та вимогам щодо дотримання протиепідемічних заходів, а також у інших ситуаціях, що передбачають відсутність можливості провадження освітнього процесу у традиційному режимі. В таких умовах на перше місце виходить організація освітнього процесу в дистанційному режимі.

В даній роботі авторами на основі отриманого протягом року досвіду при викладанні ряду дисциплін студентам кафедри телекомунікацій ІТС в дистанційному режимі пропонується відповісти на два важливих методичних питання. Чим відрізняється процедура проведення лекції в дистанційному режимі від звичайного традиційного режиму ведення лекції в аудиторії? Чи потрібна модифікація традиційної процедури проведення лекції для дистанційного режиму з метою підвищення її ефективності?

На даний час організація освітнього процесу в дистанційному режимі в КПІ ім. Ігоря Сікорського проводиться згідно «Регламенту організації освітнього процесу в дистанційному режимі» (додаток до Наказу № 7/148 від 21.08.2020 р). Згідно Регламенту п. 2.6. - Лекція у дистанційному режимі передбачає, що здобувачі отримують інформацію лекційного матеріалу через засоби телекомунікаційного зв'язку у **синхронному** режимі – коли здобувачі отримують інформацію від лектора, з можливістю ставити йому запитання в реальному часі, або у вигляді проблемного обговорення, опрацювання додаткового матеріалу або такого, що потребує уточнення (організація відео-конференцій), або в **асинхронному** режимі – коли здобувачі отримують аудіовізуальний запис лекційного матеріалу у вигляді веб-сторінок або в іншому форматі, придатному для використання в Інтернет. Лекційний матеріал повинен

бути розміщений на Платформі «Сікорський» або на іншому ресурсі та бути доступним для здобувачів.

Платформи проведення лекцій: традиційних – аудиторія, засоби відображення інформації (дошка, проектор та ін.), лектор і слухачі; дистанційних - засоби доступу до Інтернет, програмні застосування спроможні підтримувати проведення відео-конференцій для багатьох учасників, лекційний матеріал в електронному вигляді, віртуальні образи студентів та лектора.

Особливості проведення лекційних занять для спеціальності 172 – це складність матеріалу, що подається, великий об'єм і різноманітність матеріалу, поєднання вивчення програмних засобів, обладнання і мережних структур та протоколів.

Загалом, лекція - це основна форма проведення навчальних занять, призначених для засвоєння теоретичного матеріалу. Лекція є основною формою навчального процесу у вищій школі. Усний виклад предмета викладачем, а також публічне читання на яку-небудь тему. Традиційні лекції проводяться у відповідно обладнаних приміщеннях – аудиторіях для однієї або більше академічних груп студентів. Проведення лекцій в малих, середніх академічних групах дозволяє проведення спеціальних лекцій-дискусій або лекцій-бесід (діалог з аудиторією).

Основні переваги традиційного навчання це: безпосереднє особисте спілкування з викладачем, а також спілкування з іншими студентами; можливість оцінки готовності аудиторії до сприйняття матеріалу лектором і його адаптація до аудиторії; зосередженість слухачів і викладача на лекції; наявна відпрацьована роками методика лектора викладання в аудиторії.

Згідно «Вікіпедії» варто назвати і певні типові недоліки традиційної лекції:

- інформація, яку подає викладач, спрямована, в основному, на *слухову пам'ять* студента. Цей вид пам'яті досить недосконалий. Дослідження показують, що під кінець лекції з усього обсягу поданої інформації студент може відтворити лише 10-15 %;
- великі потоки слухачів (понад 50) позбавляють викладача можливості ефективно управляти розумовою діяльністю студентів;
- студенти молодших курсів слабо володіють методикою і технікою сприймання змісту лекції та конспектування;
- лекція певною мірою привчає студента до пасивного привласнення чужих думок, не стимулює тягу до самостійного навчання, не забезпечує індивідуального, диференційованого підходу до навчання.

Зручність і переваги дистанційного навчання перед іншими формами навчання полягають в наступному. Основною перевагою дистанційної форми навчання над очною формою є, передусім:

- можливість навчатися в будь-який час. Студент, який навчається дистанційно, може самостійно вирішувати, коли і скільки часу протягом семестру йому приділяти на вивчення матеріалу. Він будує для себе індивідуальний графік навчання;
- мобільність. Зв'язок з викладачами, репетиторами здійснюється різними способами: як on-line, так і off-line;
- можливість навчатися в своєму темпі. Завжди можна повернутися до

- вивчення більш складних питань, кілька разів подивитися відео-лекції, перечитати переписку з викладачем, а вже відомі теми можна пропустити;
- можливість навчатися в будь-якому місці. Студенти можуть вчитися, не виходячи з дому чи офісу, перебуваючи в будь-якій точці світу;
 - навчання в спокійній обстановці. Проміжна атестація студентів дистанційних курсів проходить в формі on-line тестів. Тому в учнів менше приводів для хвилювання перед зустріччю з викладачами на заліках та іспитах;
 - заміна конспектів електронними ресурсами та новітніми методами навчання, постійні консультації з викладачем надають цій формі освіти додаткові переваги перед очною.

Серед недоліків варто виділити:

- технічний аспект – студенти не завжди можуть мати необхідне технічне обладнання: комп'ютер або доступ в Інтернет;
- відсутність безпосереднього особистого спілкування з викладачем, а також спілкування з іншими студентами;
- психологічну і “комп'ютерну” невідповідність викладачів. Це пов'язано з традиційною методикою навчання, яка передбачає не віртуальне, а безпосереднє спілкування між студентом і викладачем;
- значні грошові витрати для університету, адже потрібно оновлювати матеріальну базу, комп'ютерну техніку, виділяти приміщення, забезпечувати доступ до Інтернет викладачів та ін.
- в Україні й досі не існує чітких технологічних можливостей автентифікації студентів;
- для дистанційного навчання потрібно мати сильну мотивацію й самоорганізацію, бо дистанційне навчання – це, передусім, самоосвіта, тобто здатність студента працювати самостійно.

Крім того, згідно проведених досліджень в Стенфордському університеті (Stanford researchers identify four causes for 'Zoom fatigue' and their simple fixes) були виявлені психологічні наслідки щоденного багатогодинного використання Zoom і інших популярних платформ для відеочатів, що призводять до стомлення людей. Це:

- занадто багато близького інтенсивного зорового контакту (така кількість зорового контакту і розмір осіб на екрані, як в чатах, неприродна для людини);
- неприродно довге споглядання свого обличчя (люди стають більш критичними до себе, коли бачать своє відображення);
- різке зниження мобільності (особисті і телефонні розмови дозволяють людям ходити і рухатися) а при відеоконференції користувачеві доводиться залишатися на одному й тому ж місці;
- підвищення когнітивного навантаження (в чатах нам доводиться старатися сильніше, щоб посилати і приймати повідомлення - людям доводиться контролювати, чи не вийшли вони з кадру, чи достатньо помітні були жести та ін.).

При переході від традиційного до дистанційного навчання може втрачатись ряд важливих факторів: контроль за аудиторією, безпосередність в спілкуванні, ідентифікація слухачів, попередня оцінка об'єму засвоєння матеріалу.

Необхідно також враховувати загальну проблему лекційних курсів, що у різного покоління студентів різне засвоювання матеріалу. Тобто, в залежності від покоління студентів змінюється сприйняття інформації - час ефективного неперервного сприйняття. Так можна розділити потоки слухачів на чотири класи часу сприйняття матеріалу лекцій:

- вступники початку 2000-2005 рр. – від 10 хв. до 40 хв.;
- вступники середини 2006-2010 рр. – від 5 хв. до 25 хв.;
- вступники середини 2011-2018 р. – від 1 хв. до 10 хв.;
- вступники 2019-2021 рр. – від 30 с до 3 хв.

Якщо не робити потокові великі академічні групи, то може бути ефективно використана форма тренінгу. Тренінгові і традиційні форми навчання мають істотні відмінності. Традиційне навчання здебільшого орієнтоване на правильну відповідь, а тренінг, насамперед, орієнтований на запитання та пошук. На відміну від традиційних, тренінгові форми навчання повністю охоплюють увесь потенціал людини: рівень та обсяг її компетентності (соціальної, емоційної та розумової), самостійність, спроможність до ухвалення рішень, взаємодії тощо. Звичайно, традиційна форма передачі знань не є сама собою чимось негативним, проте у світі стрімких змін і безперервного застарівання знань вона має звужені рамки застосування.

На тренінговому занятті перевага віддається діяльності не вчителя, а учнів, особистий досвід яких є основою для навчання. Не варто читати лекцій, буде доцільно, якщо учні поділяться тим, що знають на цей момент, і самі відшукають та/або засвоять інформацію, якої не вистачає.

Таким чином, на наш погляд для підвищення ефективності проведення дистанційного навчання потрібно здійснити: відхід від традиційного проведення лекцій. Зменшення часового неперервного подання матеріалу, ведення форми лекція-тренінг – для малих та середніх академічних груп; для поточкових (слухачів більше 50...80) лекцій ведення трансляція підготовлених записаних відео-лекцій з наступним автоматичним тестуванням слухачів; найбільш ефективна робота відеоконференцій з середніми і малими академічними групами; збільшення кількості поточних тестувань; вирішення проблеми ідентифікації слухачів – необхідне чітке положення.

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).
3. Мачинська Н.І., Стельмах С.С. Сучасні форми організації навчального процесу у вищій школі: навчально-методичний посібник / Н.І. Мачинська, С.С. Стельмах. – Львів: Львівський державний університет внутрішніх справ, 2012. – 180 с. ISBN 978-617-511-119-2.

МЕТОД БЕЗПОСЕРЕДНЬОГО ЗБОРУ ДАНИХ З ВУЗЛІВ БЕЗПРОВОДОВОЇ СЕНСОРНОЇ МЕРЕЖІ ТЕЛЕКОМУНІКАЦІЙНИМИ АЕРОПЛАТФОРМАМИ

Романюк В.А.¹, Лисенко О.І.², Романюк А.В.², Гримуд А.Г.¹

1. Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

2. Інститут телекомунікаційних систем „КПІ ім. Ігоря Сікорського”

E-mail: romval2016@gmail.com

METHOD OF DIRECT COLLECTION OF DATA FROM NODES WIRELESS SENSOR NETWORK BY TELECOMMUNICATION AIRPLATFORMS

Suggestions for improving the direct method of data collection from wireless sensor network nodes in the implementation of various targeted network management functions are considered.

Розглядається безпроводова сенсорна мережа (БСМ), вузли якої розміщені у важкодоступній або постраждалій в результаті надзвичайної ситуації території, в умовах відсутності телекомунікаційної інфраструктури загального користування. Характерними особливостями БСМ є: значна розмірність (сотні, тисячі вузлів), обмеженість ресурсів вузлів (енергії батареї, продуктивності процесора, пам'яті, потужності передавача, пропускної спроможності радіоканалу тощо). Збір інформації моніторингу з вузлів БСМ класичними методами не можливий (в умовах відсутності зв'язності між вузлами) або призводить до значних витрат енергії вузлів та малого часу функціонування мережі. В цих умовах для збору інформації моніторингу з вузлів БСМ застосовуються телекомунікаційні аероплатформи (ТА). Сенсорні вузли здійснюють моніторинг певних параметрів зовнішнього середовища або об'єктів зон свого покриття, зберігають отримані дані та чекають можливості їх передачі до ТА при її появі в зоні радіозв'язку. ТА облітають сенсорні вузли і збирають їх дані моніторингу.

Основними цільовими функціями управління при зборі даних з вузлів БСМ ТА можуть бути: мінімізація часу (граничний час) збору даних $T_{зб}$, максимізація часу (визначений час) функціонування мережі $T_{ф}$ при реалізації процесу збору даних з вузлів ТА, мінімізація кількості задіяних ТА [1, 2].

Одним з основних методів збору даних з вузлів даного класу БСМ є метод безпосереднього (прямого) збору даних ТА з кожного вузла мережі. Його основна перевага – всі задачі організації збору даних покладені на ТА (тому низька вартість сенсорних вузлів). При цьому можливі три варіанти обльоту мережі ТА: кожний вузол мережі; вся територія мережі (можливі різні способи обльоту – зигзаг, спіраль, квадрати тощо); визначені кластери мережі. Очевидно, що при неоднорідному розміщенні вузлів на площі доцільно застосовувати кластеризацію мережі, потім – здійснювати обліт ТА вузлів в цих кластерах за розрахованою траєкторією та зібрати дані моніторингу.

Відмітимо, що час збору даних ТА залежить від: кількості кластерів та їх розташування на місцевості; кількості вузлів, їх параметрів та місць розміщення в кожному кластері; кількості та положення точок збору даних ТА у просторі

кластера; вимог до якості збору даних (з гарантією збору всіх даних або без гарантії), цільових функцій управління процесом збору даних тощо.

В існуючих роботах запропоновано знаходити „центри мас” кластерів та здійснювати обліт ТА мережі тільки через центри цих кластерів, що значно скорочує час обльоту, однак ці методи не враховують можливість мінімізації кількості кластерів за рахунок адаптації до радіуса R покриття (висоти польоту) ТА, стан енергії вузлів та не впливають на час функціонування БСМ (рис. 1).

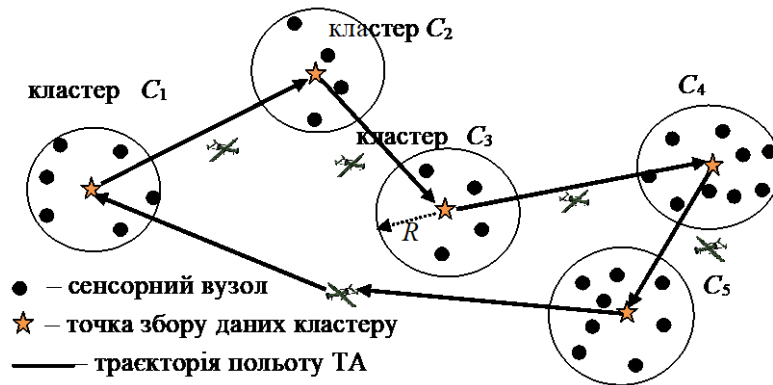


Рис. 1. Варіант переміщення ТА між точками збору даних в кластерах.

Пропонується вдосконалений метод безпосереднього збору даних моніторингу з вузлів безпроводової сенсорної мережі з їх кластеризацією телекомунікаційними аероплатформи, основними відмінностями якого є:

1. Для тимчасової кластеризації мережі в якості головного вузла кластеру запропоновано використовувати ТА, яка реалізує (на відміну існуючих центроїдних алгоритмів) модифікований ітераційний алгоритм кластерного аналізу FOREL-2 та знаходить мінімальну кількість точок збору даних в мережі та тим самим зменшує довжину маршруту обльоту (час збору).

Рішення по кластеризації може прийматися централізовано центром управління мережею (ЦУМ) при наявності інформації про стан вузлів БСМ або ТА при її відсутності в центрі управління. Центр управління мережею постійно коригує цільові функції управління в залежності від ситуації на мережі, вимог щодо якості збору даних та наявних ресурсів.

2. Рішення по траєкторії, швидкості переміщення (точки зависання) ТА в кластері, визначення цільових функцій управління і алгоритмів збору даних ЦУМ (або ТА) приймає окремо по кожному кластеру мережі.

3. Базовий маршрут обльоту точок збору даних будується за одним з відомих методів побудови найкоротшого шляху (рішення задачі комівояжера). Однак, для обльоту вузлів в кластерах запропоновані нові правила корегування базового маршруту обльоту та розроблені моделі розрахунку точок обміну між ТА і вузлами кластеру, які враховують пріоритет визначених цільових функцій управління мережею.

4. Застосування траєкторно-позиційної моделі обміну даними в радіоканалі між ТА і вузлами кластеру, яка враховує: стан вузлів (координати розташування, рівень енергії батарей, об'єм даних моніторингу); траєкторію переміщення (положення зависання) ТА; вимоги щодо забезпечення гарантії обслуговування вузлів; пріоритет цільових функцій управління.

Траєкторна модель реалізована в новому гібридному (децентралізованому/централізованому) протоколі обміну даними між вузлами і ТА (модифікація IEEE 802.11), якій складається з 4-ох основних етапів: ініціалізація обміну ТА з сенсорними вузлами кластера; передача вузлами запитів на обмін (ЗО) з ТА; складання ТА графіка передач сенсорних вузлів за правилами та моделями, які визначають точки збору ТА у просторі та послідовність передач вузлів кластеру в цих точках; безпосередньо обмін даними моніторингу вузлів з ТА.

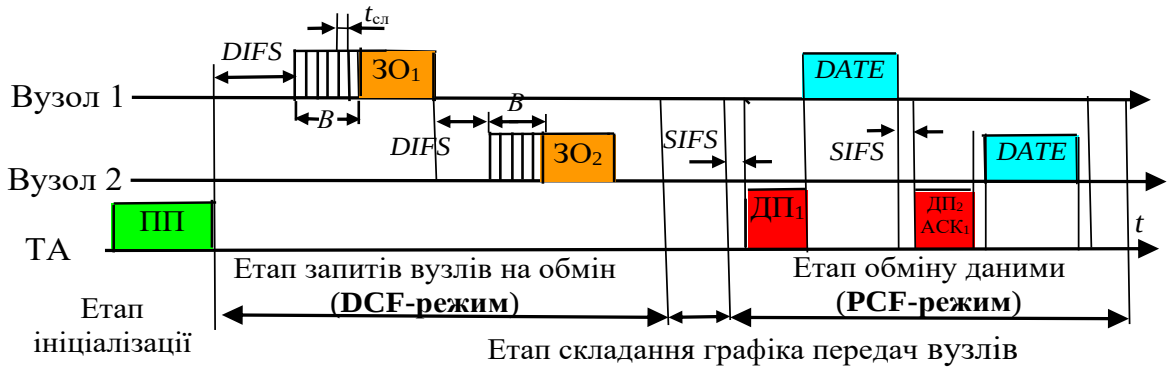


Рис. 2. Функціонування запропонованого гібридного протоколу.

Зменшення витрат енергії батарей вузлів досягається за рахунок:
визначення точок обміну на траєкторії польоту ТА, які знаходяться на найближчій відстані між вузлом і ТА;

здійснення передачі вузол-ТА з мінімальним рівнем потужності при забезпеченні необхідної швидкості обміну;

обльоту ТА перевантажених та/або „виснажених” вузлів.

Позиційна модель визначає точки збору даних ТА у просторі (для БПЛА роторного типу) кластера, які дозволяють мінімізувати загальні витрати енергії на передачу вузлів або загальний час передачі даних вузлів цього кластеру.

Для оцінки результатів функціонування алгоритму здійснена його програмна реалізація в середовищі MATLAB. Проведено експерименти і отримані залежності: часу збору даних, часу функціонування мережі від розмірності мережі, кількості вузлів в кластері, обсягу даних моніторингу при застосуванні різних методів безпосереднього збору даних.

Доведена перевага застосування вдосконаленого методу безпосереднього збору даних з вузлів БСМ ТА, якій дозволяє отримати вигоду у часі збору даних моніторингу мережі на 10 – 15% (за рахунок зменшення точок збору даних) та збільшити час функціонування мережі (за рахунок нових правил обльоту вузлів в кластерах та розрахунку точок обміну) на 12 – 17% у порівнянні з існуючими центроїдними методами безпосереднього збору даних.

Література

1. V.A. Romaniuk, O.I. Lysenko, A.V. Romaniuk, O.V. Zhuk Increasing the efficiency of data gathering in clustered wireless sensor // Information and Telecommunication Sciences, №1. – 2020. P. 102 – 107.
2. A.V. Romaniuk, V.A. Romaniuk, O.I. Lysenko, M.K. Sparavalo, O.V. Zhuk Synthesis of data collection methods by telecommunication airplatforms in wireless sensors networks// Information and Telecommunication Sciences, № 2. – 2020. P. 63 – 73.

ONTOLOGY-BASED APPROACH TO SCIENTIFIC INSTITUTIONS INFORMATION REPRESENTATION

L.S. Globa¹, R.L. Novogradska², B.O. Zadoienko¹ and Yu Junfeng³

¹ *Dept. of Infocommunication Networks, Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine*

² *Intelligent network tools department, National Center*

"Junior Academy of Sciences of Ukraine", Kyiv, Ukraine

³ *Information research institute of Shandong academy of science, Shandong, China*

E-mail: lgloba@its.kpi.ua, rinan@ukr.net, zadoenko.bogdan@gmail.com, yujf@sdas.org

ОНТОЛОГІЧНИЙ ПІДХІД ДО ПРЕДСТАВЛЕННЯ ІНФОРМАЦІЇ НАУКОВИМИ УСТАНОВАМИ

У статті представлений підхід до проектування онтологічної моделі для представлення інформації, накопиченої науковими установами. Онтологія дозволяє структурувати та систематизувати таку інформацію для подальшого використання в процесі оцінки діяльності установ. Загальна онтологія представлена системою взаємопов'язаних компонентів, кожна з яких дозволяє описати відповідний підпроцес як в рамках діяльності самої установи, так і в процесі її оцінки зовнішніми організаціями та міністерствами. Описано елементи всіх компонентів системи онтології. Практична розробка запропонованої онтологічної моделі була виконана з використанням платформи розробки онтологічних рішень TEDAOs.

INTRODUCTION. Scientific and educational activities are one of the most influential factors in the development of each country's economy. An objective analysis of the effectiveness of institutions and assessment of their functioning in terms of world and domestic science, education, economics, culture, improving the quality of human life is extremely important. It is important to obtain and analyze data in an open and transparent manner using objective methods of obtaining performance indicators.

Government agencies are complex organizational systems. They have a well developed hierarchical structure, consisting of many units and subordinate institutions. Information technology is the basis of information and analytical activities for the evaluation of such objects, and information processing is one of the most complex parts of the evaluation process. This is due to the large number of complex information flows circulating in such objects; high dynamics of change in their structure, which is due to legislative changes and the presence at each level of subjective factors; the need to take into account when processing both quantitative and qualitative information.

In the course of their operation, institutions accumulate a great deal of information (when it comes to scientific and educational organizations, such information includes scientific articles, reports, employee ratings, economic

indicators, etc.) that can be used to evaluate them according to the national criteria [1, 2]. To evaluate the effectiveness of the organization the information used is already accumulated at the level of the organization. The idea to systematize and structure such information will not only facilitate its use at the institution level, but may also enable it to be used by the relevant authorities in the process of evaluating the quality of the institution's functioning. This research proposes to use the ontology as one of the knowledge representation models to organize information of scientific institutions for its structuring and systematization, as well as for its further processing and use.

The paper describes the approach to ontological model development for the representation of information accumulated by various scientific institutions and organizations. Such an approach involves the design of the ontological model structure, the description of ontological model elements, and ontology direct development, as well as filling it with data using the appropriate environment for the ontological models development.

ONTOLOGY SYSTEM OF SCIENTIFIC INSTITUTIONS INFORMATION REPRESENTATION. The functioning of scientific organizations is associated with certain specific features that are not characteristic of other types of institutions. For example, the important indicators of the scientific process are as follows the number of publications, citations, various scientific indexes and ratings, participation in international projects and programs, completed scientific topics, trained specialists of different qualification levels in different specialties and specializations, and more. That is why the information produced during the operation of such institutions also reflects all levels (aspects) of such functioning. This feature must be taken into account when developing an ontological model. Also, several basic processes are involved in the process of organization of scientific activity: organization of activity of institution; definition of indicators by which it is possible to identify the level of performance of a certain type of activity in an institution; the existence of criteria for evaluating such indicators by which it is possible to evaluate the achievements of the organization and to determine whether its activity meets the requirements; organization of the institution's evaluation process itself.

On this basis, it is proposed that in the general ontology, several ontologies be highlighted in order to represent information accumulated by scientific institutions [3]. As a result of this selection, the overall ontology will be a system of ontologies, each describing the appropriate subprocess within both the activities of the institution itself and the process of its evaluation [4]. The system as a whole will allow both to structure and organize the information accumulated by scientific

institutions, and to organize context-independent structures for its further processing and use.

Thus ontology system is a collection of several components (Fig. 1).

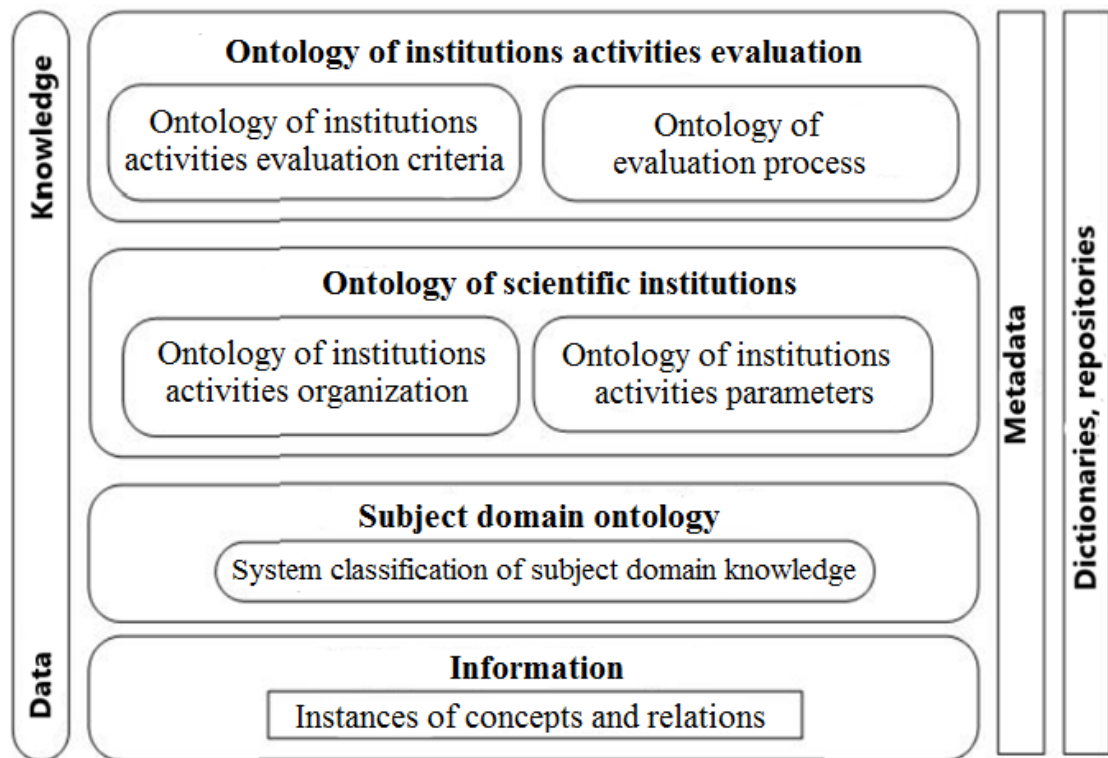


Fig. 1. Ontology system of scientific institutions information representation/

The developed system includes such ontologies as:

- Ontology of institutions activities evaluation – introduces concepts that make it possible to evaluate the effectiveness of the scientific activity of a particular scientific institution in the framework of its state review or establishment of its scientific level.
- Ontology of institutions activities evaluation criteria – sets criteria for evaluating the performance of the institution.
- Ontology of evaluation process – describes the assessment process itself by the relevant authorities.
- Ontology of scientific institutions – reflects all possible processes that occur within the scientific process within the activities of scientific institutions.
- Ontology of institutions activities organization – describes general concepts that relate to the organization of scientific activity as a whole.
- Ontology of institution activities parameters – allows to describe in detail the indicators on all aspects of the activity of the institution.
- Subject domain ontology – is based on the systematic classification of scientific activity.

Instances of classes and relations defined in an ontology form a database content that contains terms that represent the subject domain. Initial data for the knowledge representation model that characterize the subject area are various regulatory documents, as well as textbooks, manuals, periodicals, reports, information resources and more.

The practical implementation of the ontological model and its filling was performed using the Transdisciplinary Educational Dialogues of Application Ontology Systems (TEDAOS) platform. The TEDAOS platform provides many software tools for storing and processing knowledge through the development of ontologies [5, 6]. During the construction of the ontological model, 895 objects and 2837 data elements (attributes) were created.

CONCLUSIONS. Proposed ontology system will not only enable the representation of information accumulated by scientific institutions in the process of activity, but also organize structures for its further use and processing. The ontological representation allows to evaluate the quality of scientific institutions functioning on the basis of national principles for such assessment. The information how to organize the evaluation process as well as generally accepted evaluation criteria are also stored in the ontological model.

References

1. "Regulations on state certification of research (scientific and technical) institutions" [<https://zakon.rada.gov.ua/laws/show/469-98-%D0%BF/print>]
2. "Methods of optimization (certification) of budget research institutions, which are fully or partially funded by the state budget" [<https://zakon.rada.gov.ua/laws/show/1176-2011-%D0%BF/print>]
3. Globa, L., Novogrudska, R., Zadoienko, B., Junfeng, Y.: Ontology of scientific and educational institutions information. Information and telecommunication science, 2, 86-91 (2020). DOI: <https://doi.org/10.20535/2411-2976.22020.86-91>.
4. V.Yu. Velychko, M.A. Popova, V.V. Prykhodniuk, and O.E. Strizhak 2017 TEDAOS - IT platform for the formation of transdisciplinary information environments (in Ukrainian), Weap. Sys. Milit. Equip., no. 1, pp. 10-19.
5. M.A. Popova, O.E. Strizhak 2013 Ontological interface as a means of presenting information resources in a GIS environment, (in Ukrainian), Scient. Not. Taurida Nat. Univ., vol. 26(65), no. 1, pp. 127-135.

МЕТОД ПІДВИЩЕННЯ ПРОПУСКНОЇ ЗДАТНОСТІ МОБІЛЬНИХ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ НА ОСНОВІ ВИКОРИСТАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ АЕРОПЛАТФОРМ

Новіков В.І.

Інститут телекомунікаційних систем КПП ім. Ігоря Сікорського, Україна

E-mail: novikov1967@ukr.net

A method of increasing the throughput of mobile wireless sensor networks based on the use of telecommunication aerial platforms

Development of a method to increase the throughput of mobile wireless sensor networks with telecommunications aircraft in conditions of rapid and unpredictable movement of mobile sensor nodes.

Мобільні безпроводові сенсорні мережі (МБСМ) із використанням телекомунікаційних аероплатформ (ТАП) є важливою складовою системи оперативного забезпечення зв'язку підрозділів рятувальних бригад і інших служб під час надзвичайних ситуацій природного і техногенного характеру, військових конфліктів, тощо [1]. На сьогодні недостатньо розв'язаною є задача оптимального оперативного розміщення ТАП для підвищення пропускної здатності МБСМ із використанням ТАП із одночасним забезпеченням структурно-функціональної зв'язності мобільних сенсорних вузлів (МСВ). Запропоновані на сьогодні методи управління топологією (місцеположенням) ТАП, вирішують лише часткові задачі забезпечення структурної зв'язності роз'єднаних компонентів мережі і не враховують обмеження ємності каналних ресурсів, розподілу навантаження і обслуговування пакетів в вузлах мережі [2]. Отже виникає актуальна наукова задача розробки методу підвищення пропускної здатності мобільних безпроводових сенсорних мереж на основі використання телекомунікаційних аероплатформ з управлінням положенням телекомунікаційних аероплатформ в умовах швидкого і непередбачуваного переміщення мобільних сенсорних вузлів.

Розроблено новий метод підвищення пропускної здатності МБСМ на основі використання ТАП [3]. Відмінність розробленого методу від відомих полягає в тому, що вперше були об'єднані в єдину обчислювальну процедуру математичні моделі оцінки зв'язності МСВ, математичні моделі оцінки якості обслуговування МСВ і удосконалений алгоритм пошуку квазіоптимального положення ТАП. Це створює можливість досягати близьких до екстремальних значень пропускної здатності МБСМ із ТАП в умовах швидкого та непередбачуваного переміщення МСВ.

Удосконалено математичну модель оцінки зв'язності мобільних сенсорних вузлів мобільної безпроводової сенсорної мережі із

телекомунікаційним аероплатформами. Суть удосконалення математичної моделі полягає в тому, що вперше були об'єднані сукупність аналітичних моделей оцінки достовірності передачі повідомлень в радіоканалах і сукупність аналітичних моделей прогнозування переміщення мобільних сенсорних вузлів [3].

Удосконалено алгоритм пошуку квазіоптимального положення ТАП. Суть удосконалення алгоритму пошуку квазіоптимального положення ТАП полягає в тому, що при його застосуванні вдалося уникнути повного перебору варіантів розміщення ТАП в просторі завдяки використанню попередньо розробленої сукупності правил відбору варіантів зміни зв'язності МБСМ із ТАП, що підвищують пропускну здатність мережі і зменшують час обчислень [3].

Моделювання функціонування МБСМ із ТАП здійснювалося на базі комп'ютерних середовищ Microsoft Excel і Maple. Застосовувалися наступні вихідні дані: $N=165$ – кількість МСВ; $K=5$ – кількість ТАП; $r=10000 \times 10000 \text{ м}^2$ – розмір району розміщення МСВ; $d^0=600 \text{ м}$ – максимальна дальність зв'язку МСВ-МСВ; $R'=1500 \text{ м}$ – максимальна дальність зв'язку МСВ-ТАП; алгоритм пошуку найкоротших шляхів – Дейкстри; $L=1024$ біт – довжина пакету; $V=11 \text{ Мбіт/с}$ – швидкість передачі; $v_i=15 \text{ м/с}$, $i=\overline{1, N}$ – середня швидкість переміщення МСВ. Інші вихідні данні повторюють дані з попередніх розділів.

Для оцінки ефективності запропонованого методу було розглянуто наступні стратегії управління (СУ) положенням ТАП:

1. Базова стратегія управління (СУ1) з покриттям максимальної кількості МСВ.
2. Стратегія управління з використанням методу повного перебору (СУ2).
3. Стратегія управління на основі запропонованих правил (СУ3) з покриттям максимальної кількості перевантажених вузлів.

Оцінка ефективності запропонованого методу проводилася в наступній послідовності:

- 1) Задання топології МБСМ із ТАП випадковим чином та розміщення ТАП відповідно СУ1, СУ2 та СУ3 (рис. 1).
- 2) Розрахунок пропускну здатності $S(C)$ МБСМ із ТАП для кожної СУ. Визначення виграшу стратегій СУ2 і СУ3 по відношенню до СУ1 та достовірності результатів кожної СУ відносно методу повного перебору (рис.2, 3).
- 3) Розрахунок часу пошуку рішення для методу повного перебору (СУ2) і запропонованого методу (СУ3) та порівняння значень із тривалістю зв'язності МСВ.

Аналіз графіків залежності пропускну здатності МБСМ із ТАП від загального навантаження при різних стратегіях управління показує, що в діапазоні трафіку від 600 до 1500 пакетів стратегія управління положенням ТАП (СУ3) значно переважають базову стратегію (СУ1) впродовж

нормованого часу передачі пакету T . В інших діапазонах трафіку усі СУ майже однаково неефективні.

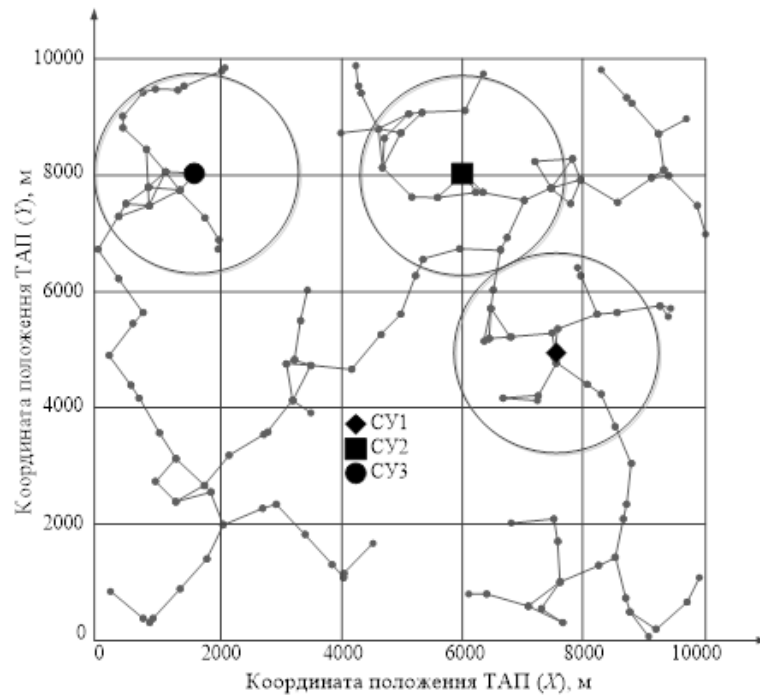


Рис. 1. Початкова топологія МБСМ із розміщенням одного ТАП для СУ1, СУ2 і СУ3.

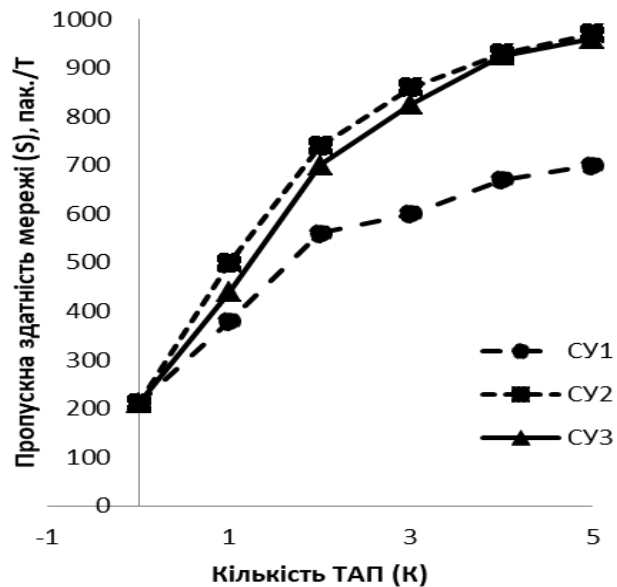


Рис. 2. Залежність ПЗ мережі для різних систем управління положенням ТАП від кількості виведених ТАП.

Оцінка ефективності запропонованого методу показує наступне:

1) Виграш запропонованого методу (СУ3) відносно базової стратегії (СУ1) при генерації 100 початкових випадкових топологій становить в середньому 10-12%.

2) Відхилення значення пропускної здатності в запропонованому методі (СУ3) від пропускної здатності в методі повного перебору (СУ2) становить в середньому 5-7%.

3) При середній тривалості зв'язності між МСВ 350с час отримання рішення для запропонованого методу (СУ3) становить в середньому 24с, що дозволяє виконувати управління положенням ТАП в режимі реального часу на відміну від методу повного перебору (СУ2), для якого час отримання рішення становить десятки хвилин.

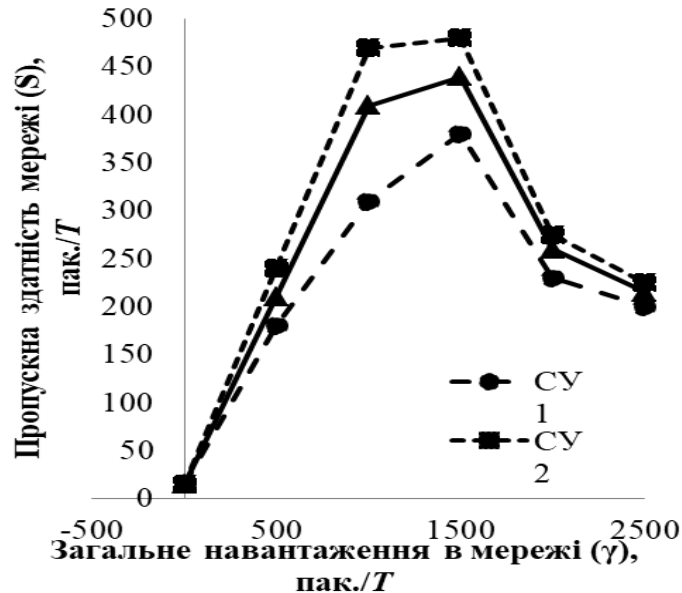


Рис. 3. Залежність ПЗ мережі для різних систем управління положенням ТАП від загального навантаження.

Практична цінність отриманих наукових результатів полягає в тому, що розроблені математичні моделі, алгоритми і метод дозволяють кількісно оцінювати вплив мобільності вузлів МБСМ із ТАП на тривалість зв'язності між МСВ; визначати раціональне положення ТАП для досягнення якомога більших значень пропускної здатності МБСМ із ТАП; здійснювати в режимі реального часу управління положенням ТАП; підвищувати ефективність систем управління мережею ТАП.

Література

1. Бунин С.Г., Войтер А.П., Ильченко М.Е., Романюк В.А. Самоорганизующиеся радиосети со сверхширокополосными сигналами. – К.: НПП «Издательство «Наукова думка» НАН Украины». – 2012. – 444 с.
2. Міночкін А.І, Романюк В.А., Жук О.В. Перспективи розвитку тактичних сенсорних мереж // Збірник наукових праць № 4. – К.: ВІТІ НТУУ «КПІ». – 2007. – С. 112 – 119.
3. Новіков В. І. Математичні моделі, методи і алгоритми оптимізації показників функціонування безпроводових сенсорних мереж із мобільними сенсорами та телекомунікаційними аероплатформами [Текст] / В.І. Новіков, О.І. Лисенко, С.В. Валуйський, О.Г. Гуйда // Вчені записки Таврійського національного університету імені В.І. Вернадського. – 2020. Том 31 (70) № 3 2020 Частина 1. – С. 54 – 64.

ПЕРСПЕКТИВИ РОЗВИТКУ ПРОЕКТУ СУПУТНИКОВОГО ЗВ'ЯЗКУ STARLINK В УКРАЇНІ

¹Ільченко М., ²Kulikov Є., ¹Кириндась Н., ¹Лісовський К.,
³Субботський Д., ¹Живков О.

¹Інститут телекомунікаційних систем КІІ ім. Ігоря Сікорського, Україна

²Технічний директор компанії «Сатлайн» (2002-2007)

³Інженер компанії «Інфоком-СК» (1990-1995)

E-mail: lisovskyi.kostiantyn@lil.kpi.ua, n.kyryndas-2027@kpi.ua

PROSPECTS FOR THE DEVELOPMENT OF THE STARLINK SATELLITE COMMUNICATION PROJECT IN UKRAINE

The report considers the technical parameters of the STARLINK satellite communication project and the prospects for its implementation and development in Ukraine. It is noted that with the expected growth of the satellite constellation in 2021 to 1000-2000 satellites, the STARLINK service will be available in Ukraine no earlier than 2022. In addition to the technical parameters of the project, much attention is paid to the organizational and legal problems associated with the licensing of similar projects in Ukraine.

В даний час, відомі кілька проектів організації мереж доступу в інтернет за допомогою так званих «низькоорбітальних» супутникових систем [1]. Однак найбільшу увагу привертає до себе проект STARLINK, який почав активно розвиватись у другій половині 2020 року - початку 2021 року:

- У вересні 2020 року SpaceX повідомила, що на початкових стадіях тестування сервісу були продемонстровані **наднизька затримка сигналу та швидкість завантаження понад 100 Мбіт/с.**

- **24 січня в 17:00 за київським часом** відбувся наймасовіший за кількістю корисних навантажень запуск в історії космонавтики. На орбіту на ракеті компанії SpaceX вийшло 143 супутника загальною масою понад п'ять тон для більш ніж 30 клієнтів від урядів, організацій, підприємств та **ВУЗів.** Серед корисних навантажень було і **10 супутників Starlink.**

- 3 січня 2021 року заплановано платну бета-версію поширити на інші континенти, починаючи з Великобританії. Згідно з інформацією від британського регулятора Ofcom, Starlink отримала ліцензію на свої широкосмугові термінали в листопаді 2020 року [2].

- 14 березня 2021 запущено чергові **60 супутників.**

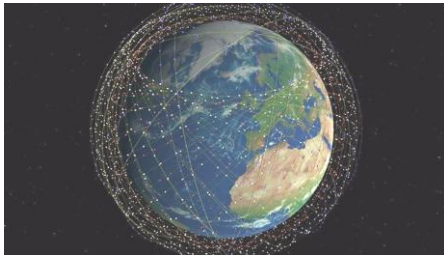


Рис. 1. Арт-зображення системи супутникового зв'язку Starlink.

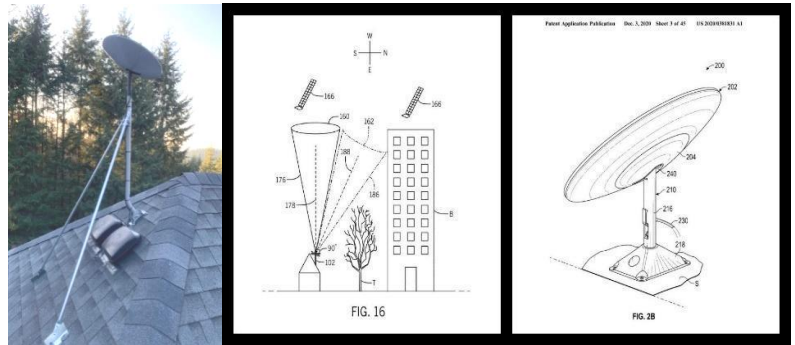


Рис. 2. Абонентська станція системи супутникового зв'язку Starlink (фото діючої станції та рис. 3 патенту [3]).

Зрозуміло, користувачів інтернет цікавлять в першу чергу швидкість передачі інформації та затримки в мережі. Однак, оскільки мова йде про систему супутникового зв'язку *Ku* діапазону частот, в якій навіть абонентська станція (рис. 2) є досить потужним (до 8 Вт) приймально-передавальним пристроєм [3]. Для порівняння - потужність звичайного стільникового телефону - близько 1-2 Вт, а точки доступу Wi-Fi – 100-200 мВт.

Систему Starlink можна розглядати як альтернативу мереж стільникового зв'язку 5G. А отже:

- Для повного розгортання 5G це обійдеться компаніям, що виробляють мобільні телефони, виробникам чіпів, пристроїв та розробникам програмного забезпечення, близько 200 млрд доларів на рік на дослідження та капітальні витрати. Космічні супутники наступного покоління могли б повністю замінити наземні опори з оптоволоконних та стільникових мереж через нижчу вартість та більш ремонтпридатну інфраструктуру.
- Є деякі підрахунки, що масове виробництво невеликих інтернет-супутників з низькою орбітою може скласти до 100000 доларів США кожен. Недорогий запуск SpaceX може зробити будівництво, заміну та модернізацію супутників Інтернету дешевшими, ніж вежі стільникового зв'язку. Також варто зазначити, стільникові вежі мають витрати на оренду землі.
- Мережа що містить від 4000 до 12000 Інтернет-супутників може складатись з понад 500000 космічних апаратів. Цілу космічну мережу з 500000 можливо замінити за 60 мільярдів доларів.

Питання в тому, чи потрібно будувати в Україні шлюзову станцію Starlink (рис. 3) – це не тільки економічне, але й стратегічне питання з точки зору державної безпеки, пов'язане з тим, як і яким чином буде спрямовуватись та регулюватись супутниковий трафік державних установ, шкіл, міністерств і відомств. Цілком очевидно, що однією з головних «дійових осіб» у вирішенні цієї проблеми буде «Мінцифри», яке вже декларувало своє бачення використання проекту Starlink в Україні.

Однак не лише технічні та економічні параметри Starlink будуть впливати на перспективи її використання в Україні. Вагому роль також відіграватиме законодавство нашої Держави в області ліцензування послуг зв'язку і використання радіочастот. Справа в тому, що система Starlink працює в так званому *Ku* діапазоні частот [5], в якому в Україні вже реалізовувались проекти будівництва мереж супутникового зв'язку типу VSAT (таблиця 1).

Табл. 1. Смути частот, що використовуються в системі SpaceX [6].



Рис. 3. Шлюзові (Gateway) системи Starlink.

Type of Link and Transmission Direction	Frequency Ranges
User Downlink Satellite-to-User Terminal	10.7 – 12.7 GHz
Gateway Downlink Satellite to Gateway	17.8 – 18.6 GHz 18.8 – 19.3 GHz
User Uplink User Terminal to Satellite	14.0 – 14.5 GHz
Gateway Uplink Gateway to Satellite	27.5 – 29.1 GHz 29.5 – 30.0 GHz
TT&C Downlink	12.15 – 12.25 GHz 18.55 – 18.60 GHz
TT&C Uplink	13.85 – 14.00 GHz

На сьогоднішній день послідовність дій суб'єкта господарювання для отримання ліцензії на користування радіочастотним ресурсом України виглядає наступним чином [7]:

1. Відповідно до частини 2 статті 30 Закону України "Про радіочастотний ресурс України" визначитись яким він є користувачем радіочастотного ресурсу (подальші дії визначені лише для суб'єктів господарювання, які користуються радіочастотним ресурсом України для надання телекомунікаційних послуг і включені до Реєстру операторів і провайдерів) [8].

2. Відповідно до Національної таблиці розподілу смуг радіочастот України та Плану використання радіочастотного ресурсу України визначити радіотехнологію та смуги радіочастот [9].

3. Відповідно до ст. 42 Закону України "Про телекомунікації" та рішення НКРЗІ від 01.11.12 № 560 подати до НКРЗІ заяву про включення до реєстру операторів, провайдерів телекомунікацій [10].

4. Відповідно до Ліцензійних умов користування радіочастотним ресурсом України та статті 32 Закону України "Про радіочастотний ресурс України" підготувати заяву та пакет документів для отримання ліцензії.

5. Направити цінним листом з описом вкладення документи на адресу НКРЗІ, або подати особисто.

6. У разі залишення заяви без розгляду, суб'єкт господарювання може усунути виявлені недоліки та повторно подати заяву та пакет документів на новий розгляд.

7. Після прийняття НКРЗІ рішення про видачу ліцензії на користування радіочастотним ресурсом України та отримання листа-повідомлення про розмір плати за видачу ліцензії суб'єкт господарювання, не пізніше 30 календарних днів від дня направлення листа повідомлення, здійснює оплату визначеної суми до Державного бюджету України на рахунок місцевого відділення Державного казначейства України за кодом бюджетної класифікації **22011400**.

8. Направити по факсу до відділу ліцензування РЧР копії платіжного доручення та довідки місцевого відділення Державного казначейства України про зарахування коштів до Державного бюджету України в повному обсязі. Надходження зазначених документів є підставою для підготовки бланку ліцензії.

9. Ліцензія видається представнику суб'єкта господарювання, який зазначений у

дорученні суворой звітності, особисто на підставі наданих оригіналів документів: платіжного доручення, довідки місцевого відділення Державного казначейства України про зарахування коштів до Державного бюджету України, доручення на отримання матеріальних цінностей.

10. Після отримання першого дозволу на експлуатацію за ліцензією **поінформувати НКРЗІ про початок освоєння** радіочастотного ресурсу за ліцензією.

11. Після отримання дозволу на експлуатацію в останньому регіоні за ліцензією або на всі номінали радіочастот зазначені в ліцензії **поінформувати НКРЗІ про повне освоєння** радіочастотного ресурсу за ліцензією.

Варто зазначити, що вартість, складність і тривалість процедур отримання дозволів на ввезення, сертифікацію та ліцензування, так само як і вартість використання радіочастотного ресурсу, можуть значно вплинути на вартість послуг проекту Starlink в Україні і будуть значно відрізнятися від тих, які сьогодні декларують деякі оператори зв'язку.

Для того, щоб послуги Starlink стали доступні в Україні, варто в першу чергу на законодавчому рівні спростити процедури сертифікації і ліцензування користувацьких терміналів, в ідеальному випадку спростивши їх до рівня, який використовується в інших країнах, які вже дозволили використання таких терміналів (на прикладі згаданих вище США, Канади, Великобританії...).

В КПІ створена робоча група, до складу якої входять викладачі, співробітники і студенти Інституту телекомунікаційних систем, а також колишні випускники КПІ, які працюють в проектах супутникового зв'язку «Инфоком-СК», «Романтіс-Україна», «Сатлайн», «Глобалстар», Державному космічному агентстві України. Деякі з них працюють у профільних телекомунікаційних компаніях США і Канади і тому отримують можливість працювати з користувацькими терміналами вже навесні цього року.

Література

1. Xin Yang. Low Earth Orbit (LEO) Mega Constellations – Satellite and Terrestrial Integrated Communication Networks. Institute for Communication Systems Faculty of Engineering and Physical Sciences University of Surrey Guildford, Surrey GU2 7XH, UK November 2018.
2. Регуляторний орган у сфері медіа Великої Британії [Електронний ресурс] – Режим доступу до ресурсу: https://www.ofcom.org.uk/__data/assets/pdf_file/0020/210971/starlink.pdf.
3. SpaceX Starlink Patent Documents [Електронний ресурс] – Режим доступу до ресурсу: <https://www.tesmanian.com/blogs/tesmanian-blog/starlink-patent>.
4. How does Starlink work anyway? [Електронний ресурс] – Режим доступу до ресурсу: <https://hackaday.com/2020/02/20/how-does-starlink-work-anyway/>.
5. Заявка на фіксовану супутникову службу холдингів космічних досліджень FCC.report [Електронний ресурс] – Режим доступу до ресурсу: <https://fcc.report/IBFS/SAT-LOA-20161115-00118>.
6. SpaceX негеостаційна супутникова система FCC.report [Електронний ресурс] – Режим доступу до ресурсу: <https://fcc.report/IBFS/SAT-LOA-20161115-00118/1158350>.
7. Послідовність дій для отримання ліцензії на користування РЧР - НКРЗІ [Електронний ресурс] – Режим доступу до ресурсу: <https://nkrzi.gov.ua/index.php?r=site/index&pg=67&language=uk>.
8. Закон України «Про радіочастотний ресурс України» [Електронний ресурс] – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/1770-14#Text>.
9. Постанова КМУ «Про затвердження Національної таблиці розподілу смуг радіочастот України» [Електронний ресурс] – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/1208-2005-%D0%BF#Text>.
10. Закон України «Про телекомунікації» [Електронний ресурс] – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/1280-15#Text>.

Секція 1. Достовірне передавання сигналів та інформації в телекомунікаційних системах

УДК 621.39

АНАЛІЗ ПОБУДОВИ МЕРЕЖ ДОСТУПУ НА ОСНОВІ СУЧАСНИХ ШИРОКОСМУГОВИХ ТЕХНОЛОГІЙ

Вістунов В.Д., Гаттуров В.К.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: 99vvd@ukr.net; gvk51@bigmir.net

ANALYSIS OF CONSTRUCTION OF ACCESS NETWORKS ON THE BASIS OF MODERN BROADBAND TECHNOLOGIES

Modern networks offer a wide range of technologies for connecting subscribers to the Internet, which are divided into wireless and wired access technologies. This work is designed to answer the question: which of the modern broadband access technologies is optimal when building a network in a given situation.

В сучасних мережах існує великий асортимент технологій підключення абонентів до мережі інтернет, які поділяються на технології бездротового і дротового доступу. Ця робота покликана дати відповідь на питання: яка з сучасних технологій широкосмугового доступу є оптимальною при побудові мережі у тій чи іншій ситуації.

Будівництво мереж доступу на даний час, головним чином йде за чотирма напрямками:

- мережі на основі існуючих мідних телефонних пар і технологія xDSL;
- гібридні волоконно-коаксіальні мережі;
- бездротові мережі;
- волоконно-оптичні мережі.

Використання технологій xDSL, що постійно вдосконалюються - найпростіший і недорогий спосіб збільшення пропускної спроможності існуючої кабельної системи на основі мідних кручених пар. Для операторів такий шлях є найбільш економічним і виправданим, коли потрібно забезпечити швидкість до 10 Мбіт / с. Однак, швидкість передачі до десятків мегабіт в секунду на існуючих кабельних системах, з урахуванням великих відстаней (до декількох км) і низької якості міді, представляється непростим і більш дорогим рішенням.

Інше традиційне рішення - гібридні волоконно-коаксіальні мережі (HFC, hybrid fiber-coaxial). Підключення безлічі кабельних модемів на один коаксіальний сегмент призводить до зниження середніх витрат на побудову інфраструктури мережі в розрахунку на одного абонента і робить привабливим такі рішення. В цілому ж тут зберігається конструктивне обмеження по смузі пропускання.

Технологія FTTx – це одне з швидкісних і надійних засобів доступу в інтернет. Дане з'єднання є оптимальним для роботи великої компанії, для забезпечення стабільного підключення до мережі для підтримки роботи

цифрової телефонії, відправки та отримання великих обсягів даних, наприклад, відеозаписів, а також безлічі інших корпоративних завдань (рис.1):

- FTTN (Fiber-to-the-Home) - оптоволокно підведено безпосередньо в ваш будинок / квартиру;
- FTTB (Fiber-to-the Building) - оптоволокно підходить до будівлі, а далі розподіляється по квартирах за допомогою інших технологій (наприклад, Ethernet);
- FTTCab (Fiber-to-the-Cabinet) – волокно у розподільчу шафу;
- FTTN (Fiber-to-the-Node) – волокно до вузла.

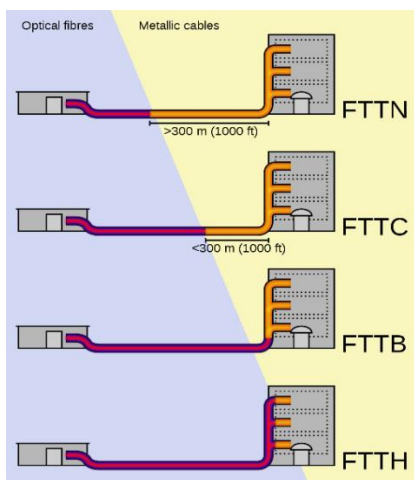


Рис.1 Підключення до мережі за технологією FTTx.

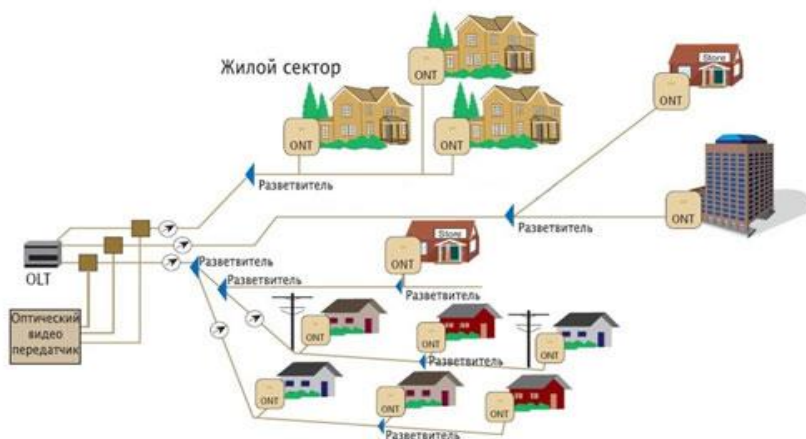


Рис.2. Принцип роботи технології PON.

Аналізуючи переваги і недоліки даної технології, можна зробити висновок, що реалізація вимагає значно більших інвестицій, ніж побудова DSL-інфраструктури, оскільки для надання високошвидкісного каналу (до декількох Гбіт / с) необхідно в багато разів збільшити пропускну здатність опорних мереж, протягнути оптоволокно до об'єктів, розробити чимало нових додатків.

PON (Passive optical network) - технологія пасивних оптичних мереж. Принцип роботи технології PON (рис.2): між приймально-передавальним модулем центрального вузла OLT і віддаленими абонентськими вузлами ONT створюється повністю пасивна оптична мережа, що має топологію дерева. У проміжних вузлах дерева розміщуються пасивні оптичні розгалужувачі (спліттери) - компактні пристрої, які не потребують живлення і обслуговування. Один приймально-передавальний модуль OLT дозволяє передавати інформацію безлічі абонентських пристроїв ONT. Число ONT, підключених до одного OLT, може бути настільки великим, наскільки дозволяє бюджет потужності і максимальна швидкість приймально-передавальної апаратури.

Технологія бездротової абонентської лінії має кілька переваг у порівнянні з альтернативними технологіями доступу. Бездротові лінії можуть бути розгорнуті в тих місцях, де через неможливість проведення робіт, щільності або «давнини» забудови просто не може бути прокладена кабельна лінія. По-друге, для певних відстаней і розташування населених пунктів

організація бездротового доступу може бути просто набагато економічно ефективнішою в порівнянні з альтернативними технологіями. Тут необхідно враховувати і витрати праці, і довжину абонентської лінії. Вартість кабельних систем в значній мірі залежить від відстані між будівлями і від ступеня концентрації груп абонентів. У той же час вартість бездротових систем залежить в основному від вартості абонентського обладнання, яке має тенденцію до здешевлення, паралельно з удосконаленням технологій. Розглянемо два приклади технологій бездротового доступу:

Технологія Wi-Fi призначена для організації невеликих бездротових мереж у приміщеннях і побудови бездротових мостів;

Технологія LTE (4G) - стандарт широкопasmового бездротового зв'язку. Мережі четвертого покоління покликані замінити собою застарілі стандарти UMTS і HSDPA (3G). Стандарт LTE на фізичному рівні використовує технологію OFDMA для передачі даних, протокол IP використовується на мережевому рівні. LTE забезпечує можливість створення високошвидкісних систем стільникового зв'язку, які оптимізовані для пакетної передачі даних.

Висновки. Аналізуючи переваги і недоліки технологій підключення абонентів до мережі інтернет, в даній роботі, показано які з сучасних технологій широкопasmового доступу є оптимальними при побудові мережі у тій чи іншій ситуації.

ADSL спочатку орієнтувалася на використання телефонних абонентських пар. Успіх цієї технології багато в чому пов'язаний з ефективною методикою суміщення звичайної телефонної мережі і мережі ADSL - найпростіший і недорогий спосіб збільшення пропускної спроможності існуючої кабельної системи на основі мідних кручених пар. Приклад масштабного використання в Україні - Укртелеком.

Інша традиційне рішення по використанню старої провідний коаксіальної інфраструктури (оператор Воля) - HFC. Однак, як і в технологіях ADSL, зберігається обмеження по смузі пропускання.

Сучасні оператори, що будують провідні мережі доступу в Інтернет, використовують технології PON, які володіють необхідною ефективністю нарощування мережі, і пропускної здатності, в залежності від справжніх і майбутніх потреб абонентів.

Бездротові мережі доступу, перш за все LTE, забезпечують можливість створення високошвидкісних систем стільникового зв'язку, які оптимізовані для пакетної передачі даних.

Література

1. Бакланов И.Г. NGN: принципы построения и организации. – М.: Эко-Трендз, 2008. – 400 с.
2. Телекоммуникационные системы и сети. Том 3. – Мультисервисные сети / Под ред. Шувалова В.П. – М.: Горячая линия-Телеком, 2005 – 592 с.
3. Hi-Tech новинки, гаджеты, новые технологии, электроника, робототехника. Интернет. Беспроводной интернет через Wi-Fi роутер /Материал взят с <http://gadgettoday.ru/259-besprovodnoj-internet-cherez-wi-fi-router.html>.
4. Рекомендація МСЭ-Т G.983.1 «Оптические системы широкопasmового доступу, що базуються на пасивній оптичній мережі (PON)». <file:///C:/Users/VALIEN/AppData/Local/Temp/T-REC-G.983.1-200501-I!!PDF-R.pdf>.

ДОСЛІДЖЕННЯ ПРОДУКТИВНОСТІ МЕРЕЖІ NGN НА БАЗІ IMS ПРИ ПЕРЕДАЧІ ТРАФІКУ МЕРЕЖІ ЗКС №7 ЗА УМОВИ ВТРАТИ ПАКЕТІВ ПРИ ВИКОРИСТАННЯМ ПРОТОКОЛІВ UDP ТА SCTP

Мещерінов М.В., Гаттуров В. К.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: mmieshch@gmail.com

INVESTIGATION OF PERFORMANCE OF NGN NETWORK ON THE BASIS OF IMS IN CASE OF TRANSFER ZKS №7 NETWORK TRAFFIC UNDER CONDITIONS OF PACKAGE LOSS USING UDP AND SCTP PROTOCOLS

This article shows the efficiency of the UDP and SCTP protocols as transport protocols in the transmission of traffic of the ZKS №7 network over the NGN network based on IMS for packet loss.

Ця стаття показує ефективність роботи протоколів UDP та SCTP як транспортних протоколів при трансляції трафіку мережі ЗКС №7 через мережу NGN на базі IMS за втрати пакетів.

IMS проектувалася в рамках мережі 3G, яка повністю базується на IP. Основним її протоколом є SIP, що дозволяє встановлювати однорангові сесії між абонентами і використовувати IMS лише як систему, яка надає сервісні функції з безпеки, авторизації, доступу до послуг і т.д. Функція управління шлюзами, як і сам медіашлюзи тут лише засіб для зв'язку абонентів 3G з абонентами фіксованих мереж. Причому маються на увазі лише ТМЗК, які функціонують на протоколі ЗКС7.

SIP (Session Initiation Protocol), розроблений IETF для VoIP-сигналізації, є протоколом управління зв'язком, здатний працювати на різних транспортних рівнях, наприклад, TCP, UDP або SCTP.

В даному дослідженні вивчався показник ефективності роботи мережі SIP при передачі трафіку мережі ТМЗК, за умови використання двох різних транспортних пакетів. Об'єктом дослідження є показники затримки трафіку при різній кількості втрачених пакетів.

На рисунку 1 показана топологія мережі, яка була використана для моделювання. Вузли 1 і 2 є маршрутизаторами з обмеженим буфером. Вузли 4 і 5 - це джерело TCP і потік, відповідно, що несуть трафік FTP, що використовується в конкретному сценарії. Вузли 0 і 3 імітують об'єкти SIP (а саме MCG), що обмінюються повідомленнями SIP в активному сеансі. Зв'язок між вузлами 1 і 2 є єдиним вузьким місцем для трафіку відом з обох кінцевих точок відправника 0 і 4, що конкурує у відповідному експерименті. Оскільки реальний сценарій може включати більшу кількість проміжних стрибків, пропускна здатність на вузькому місці вибирається для забезпечення значущих спостережень. Значення затримок вибираються таким чином, щоб загальна затримка становила 45 мс, що представляє затримку

передачі між SIP-сервером у США та іншим десь у Європі.

Модельований випадок обміну повідомленнями SIP включає проблеми з перевантаженнями та конкуренцією на шляху руху, оскільки він передає сигнали ТМЗК через IP без участі будь-якої кінцевої точки, яка знаходиться на IP. Генерування трафіку досягається за допомогою стаціонарної моделі Poission (зазвичай використовується для телефонії), що генерує SIP-повідомлення розміром 578 байт у вузлі 0.

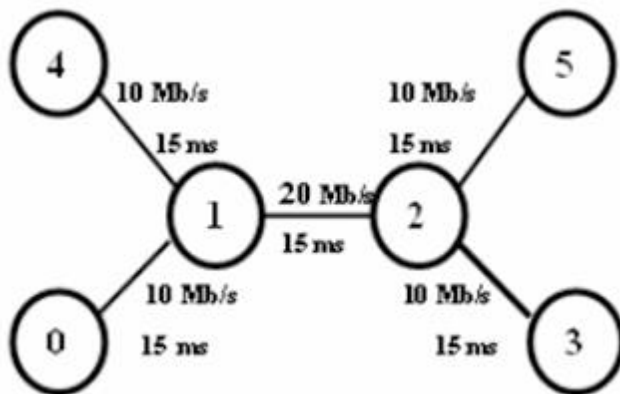


Рис. 1: Топологія мережі.

Запроси INVITE, що надходять у вузол 0, переадресовуються у вузол 1, на що спочатку поступає відповідь 100, а пізніше 180. Відповідь дзвінка повертається, коли дзвінок отримано з домену ТМЗК. Запити формуються зі швидкістю 10 Мб/с, що даватиме половину від загальної швидкості. Це пов'язано з тим, що у випадку SIP-T MGC не тільки може надіслати запити INVITE, але й ACK/200OK, тому швидкість генерації трафіку додатків подвоюється, і становитиме 20 Мб/с.

Основним спостереженням є затримка INVITE та відповідна реакція дзвінка з використанням UDP та SCTP за різних умов.

Для аналізу затримок, запропонованих транспортними протоколами, моделюються три базових сценарії. Один - вивчає вплив перехресного трафіку на затримку доставки повідомлення, другий - показує вплив різних умов втрати пакетів на затримку доставки повідомлення, а третій показує зміну пропускну здатності при зміні розміру буферу обміну на вузлі.

Для дослідження продуктивності протоколів UDP і SCTP при конкуруючому трафіку був узятий трафік протоколу TCP, з яким трафік досліджуваних протоколів зустрічається у вузлі 3, та визначено затримку проходження пакетів протоколів UDP і SCTP.

За результатами даного дослідження видно, що у випадку UDP затримки залишаються незмінними, що є основним атрибутом UDP. Він показує великі смуги затримок лише у випадку повторної передачі пакетів, які потрібно було повторно передавати. Протокол SCTP справді стикається з ситуацією, коли пакети бачать затримку до 800 мс з невеликою кількістю послідовності, проте на досить короткий час.

Для порівняння продуктивності UDP і SCTP в умовах втрати пакетів зроблено три моделювання як для UDP, так і для SCTP. У вузлі 1 моделюються випадкові коефіцієнти втрати пакетів 0,1, 0,2 та 0,3%.

Основна відмінність тут у сценарії SIP-T та проксі-сервері SIP полягає в тому, що у проксі-сервері SIP єдиним повідомленням, надісланим від кінця відправника, є INVITE, і воно отримує попередні відповіді "Trying" та "Call" від одержувача, тоді як у випадку SIP-T всі повідомлення SIP щодо встановлення, управління та припинення сеансів обробляються MGC. Отже, звичайним

повідомленням в доповнення до INVITE є ACK/200OK. Втрата ACK/200OK призведе до того, що SCTP зазнає більших затримок, оскільки втрата пакетів збільшується, а вікно перевантажень страждає все більше і більше. Для того, щоб вмістити ці пакети, вони скидаються на транспортний шар, що тоді стає справжнім ударом по продуктивності.

Третій експеримент призначений для визначення пропускної здатності, досягнутої протоколами UDP та SCTP, при імітуванні безперервного ефекту перехресного трафіку. Також в даному експерименті змінними були значення буферу обміну, при яких брались результати пропускної здатності, та які були рівні 5, 20, 50, 100, 150, 200 та 250.

Результати даного дослідження показали, що у випадку протоколу UDP пропускна здатність тримається на високому рівні, і не залежить від зміни розміру буферу обміну. У випадку протоколу SCTP чітко показана залежність пропускної здатності від розміру буферу обміну. Чим більший буфер обміну, тим більша пропускна здатність протоколу SCTP.

Висновки. Для забезпечення своєї роботи протокол SIP може використовувати різні транспортні протоколи, серед яких є досить популярними та вживаними протоколи UDP та SCTP. Кожен з цих протоколів має ряд переваг та недоліків, і може бути використаний для вирішення задачі передачі повідомлень сигналізації між підсистемою ISUP та мережею NGN на базі IMS. В даному дослідженні було проведено моделювання декількох випадків транспортування повідомлень сигналізації з різними типами обмежень, задля визначення більш відповідного протоколу для вирішення поставленої задачі.

Пропускна здатність, надана SCTP, суттєво залежить від розміру буфера, і зменшення розміру буфера значно погіршує продуктивність, пропоновану SCTP. З іншого боку, UDP виділяється навіть при розмірі буфера 5 пакетів, що чітко показано в експерименті.

Згідно результатів дослідження, у випадку конкуруючого трафіку обидва протоколи мають приблизно рівну затримку. Але при наявності малого розміру буфера або рівня втрат вищого за 0,1% пакетів, що може бути досить вірогідною ситуацією при експлуатації реальних мереж зв'язку, протокол SCTP має значно гірші показники продуктивності за протокол UDP.

Отже, виходячи з даних, отриманих за результатами цього дослідження, можна зробити висновок, що у випадку використання протоколу SIP-T як основного протоколу для вирішення задачі сигналізації підсистеми ISUP та мережі NGN, протокол UDP залишається найпродуктивнішим протоколом для передачі SIP-повідомлень.

Література

1. Гольдштейн А.Б., Гольдштейн Б.С., SoftSwitch СПб.: БХВ, Санкт-Петербург, 2006, 368 с.:
2. Бакланов, И. Г. NGN: принципы построения и организации / под ред. Ю. Н. Чернышова. – М.: Эко-Трендз, 2008. – 400 с.: илл.
3. Керівництво по TCP в системі NS-2 (електронний ресурс). Режим доступу: <http://www.ce.chalmers.se/~fccla/tcp-tour.html>.
4. Офіційне керівництво користувача системою NS-2 (електронний ресурс). Режим доступу: <http://www.isi.edu/nsnam/ns/ns-documentation.html>.

ВИКОРИСТАННЯ АУТЕНТИФІКАЦІЇ В МЕРЕЖІ ЯК СПОСОБУ ВИКОНАННЯ БЕЗПЕЧНИХ ХМАРНИХ ОБЧИСЛЕНЬ

Григоренко О.Г., Полікарпова Ю.Г.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

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

NETWORK AUTHENTICATION USING AS A WAY TO PERFORM SECURE CLOUD COMPUTING

The main authentication methods in the network are analysed, this allow to use cloud storage and perform cloud computing safely with the growing potential threats of data theft of organizations.

Проаналізовані основні методи аутентифікації в мережі, що дозволяють безпечно використовувати хмарні сховища та виконувати хмарні обчислення при зростанні потенційних загроз крадіжок даних організацій

Процес аутентифікації в мережі служить захистом від різного роду атак, метою яких є крадіжка даних у хмарному середовищі. Хмарні обчислення здебільшого використовуються різними організаціями в багатьох комерційних сферах. Постачальники хмарних послуг відповідають за ідентифікацію та інші види управління в хмарному середовищі. Однак велика кількість випадків витоку даних спричинена вразливістю в системах управління ідентифікацією. Методи аутентифікації підтверджують ідентифікацію користувача перед тим, як дати дозвіл на доступ до ресурсів. Процес аутентифікації зазвичай виконується програмним забезпеченням або його частиною. Приклад процесу аутентифікації показаний на рис.1. Хмарна система виконує один або поєднання зазначених нижче методів аутентифікації.

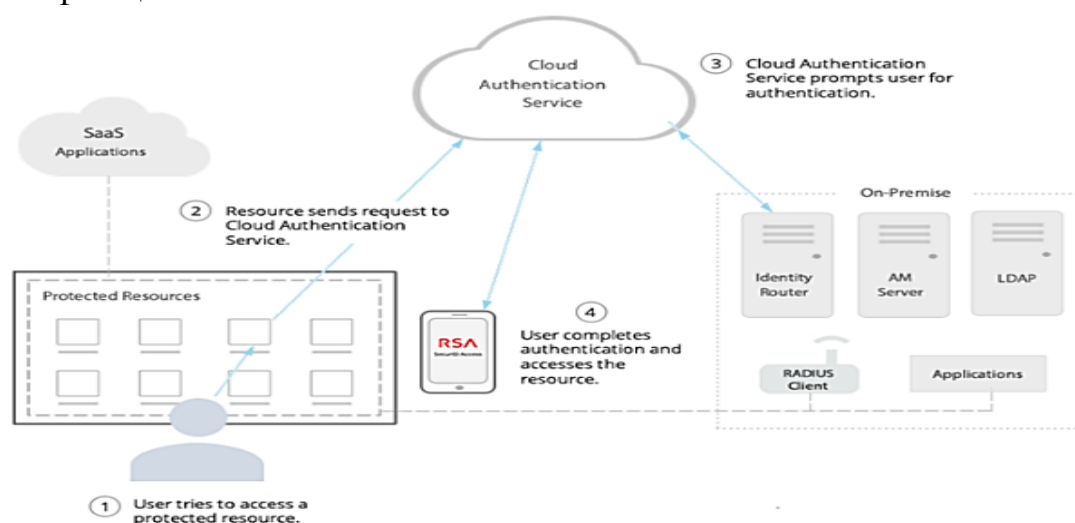


Рис.1. Приклад процесу аутентифікації в хмарному середовищі [4].

Картки доступу та біометрична аутентифікація: розпізнавання райдужки або сітківки ока, розпізнавання відбитків пальців, розпізнавання обличчя та розпізнавання долоні, забезпечують безпеку хмарних ресурсів та засобів, забороняючи несанкціонований доступ. Хмарні центри обробки даних (Cloud data centers - CDC) концентрують усі сервери, мережі та програми, щоб користувачі мали доступ до даних у будь-який час і з будь-якого місця. Для запобігання витоку даних з боку інсайдерів або будь-якого несанкціонованого доступу до CDC фізична безпека необхідна разом із певними політиками використання та управління.

Для виконання безпечних хмарних обчислень важливими є ідентифікаційні дані, які підтверджують повноваження, статус, права та права доступу. Використання таких облікових даних, як одноразовий пароль, шаблон та капча, є традиційним способом захисту системи від зловмисних дій. Найбільш часто використовуваними механізмами управління обліковими даними доступу для хмарного середовища є технології Lightweight Directory Access Protocol (LDAP) та Microsoft Active Directory (AD). Серверами LDAP та AD керують сторонні постачальники або в рамках організаційної мережі хмарних обчислень. Витрати на хмарне обслуговування збільшуються, коли на цих традиційних механізмах управління обліковими даними розгортається кілька програм. Дуже важливо додавати, вимикати, змінювати або видаляти облікові записи кожного разу, коли працівник виходить або входить в організацію. При управлінні обліковими даними на стороні провайдера виникає вразливість скидання облікових даних, коли використовуються слабкі механізми відновлення пароля. Хакери можуть відслідковувати, обробляти або компрометувати облікові дані. Ключі захищеної оболонки (Secure Shell keys - SSH) допомагають ідентифікувати сервер SSH за допомогою криптографії з відкритим ключем або аутентифікації виклику-відповіді. Головною перевагою ключів SSH є те, що аутентифікація на сервері виконується без передачі пароля по мережі. Це запобігає перехопленню або зламу пароля хакерами. Спроби вгадати облікові дані за допомогою атак грубої сили усуваються ключами SSH. Агенти SSH допомагають встановити зв'язок із серверами без використання окремих паролів для кожної системи. Агент SSH зберігає приватні ключі та надає їх клієнтським програмам SSH. Ці приватні ключі зашифровані паролем фразою, яка надається під час кожної спроби з'єднання з сервером. У кожному окремому виклику SSH паролем фрази необхідні для дешифрування приватного ключа перед тим, як перейти до фази аутентифікації. Парольна фраза використовується лише під час додавання приватних ключів до сховища агента. Основна проблема ключів SSH полягає в тому, що ключі можуть бути недостатньо захищені. Ідентифікаційні дані та ключові механізми SSH зазвичай використовуються для аутентифікації хмарних веб-служб [1].

Багатофакторна аутентифікація – ще один метод захисту цифрових активів та транзакцій через Інтернет. Як правило, одноразові паролі (One-Time Password - OTP), капчі або шаблони використовуються як вторинний механізм аутентифікації разом із ідентифікаційними даними.

Багатофакторність забезпечує додатковий рівень безпеки над традиційною аутентифікацією на основі ідентифікаційних даних. Як правило, онлайн-транзакції аутентифікуються за допомогою одноразових паролів. При фінансових операціях через Інтернет сервер за певними алгоритмами генерує одноразовий пароль, який надсилається користувачеві або через зареєстрований номер мобільного телефону, або електронною поштою. Інший тип ОТР генерується за допомогою апаратних/програмних генераторів маркерів, який захищений персональним ідентифікаційним номером (PIN). Цей пароль можна використовувати один раз, і він має певний термін використання. Капчі зазвичай використовуються для захисту веб-програм від атак зловмисного програмного забезпечення. Капча може бути буквенно-цифровою комбінацією, математичним рівнянням або зображенням. [2]

Безпека механізмів чіпа та PIN-коду полягає у використанні відкритих та приватних ключів для асиметричного шифрування та дешифрування даних. Мікропроцесорний чіп зберігає дані користувача та ключі безпеки шляхом створення унікальних даних про фінансові транзакції для захисту від шахрайства [1,3]. Зв'язок між клієнтом/терміналом із сервером аутентифікації шифрується та підписується за допомогою ключа безпеки, який зберігається в мікросхемі. Сервер перевіряє підпис і розшифровує зв'язок за допомогою ідентичних ключів, які зберігаються на сервері. PIN-код використовується для аутентифікації клієнта/терміналу для доступу до даних.

Метод єдиного входу (Single Sign-On-SSO) допомагає хмарним користувачам використовувати один пароль для доступу до всіх додатків/послуг, зберігаючи по одному обліковому запису для кожного користувача. Користувачам не потрібно вказувати свої облікові дані під час кожного доступу до різних хмарних веб-служб.

Підсумовуючи, зазначимо, що найбільш цінним ресурсом в хмарних обчисленнях є дані користувачів. Захист даних користувача вкрай важливий і значущий. Тому рішення щодо безпеки в цій системі постійно оновлюються. Важливою частиною безпеки даних у хмарі є аутентифікація. Проаналізовані методи біометричної, багатофакторної аутентифікації, використання ідентифікаційних даних, ключів SSH, механізмів чіпа та PIN-коду, методу єдиного входу дозволяють різним організаціям в багатьох комерційних сферах безпечно використовувати хмарні сховища та безпечно виконувати хмарні обчислення.

Література

1. ISSN: 2277 128X: International Journal of Advanced Research in Computer Science and Software Engineering/ [Електронний ресурс] – Режим доступу: <http://www.ijarcsse.com/>.
2. Воронцов А. В., Газизова Э.Р., Веденьев Л.Т., Афанасьев А. Н. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. – Учебное пособие для вузов, – 2009 г., 278 – 301 с.
3. Бердник А. Угрозы облачных вычислений и методы их защиты [Електронний ресурс] / Алексей Бердник. – 2013. – Режим доступу до ресурсу: <https://habr.com/ru/post/183168/>.
4. RSA SecurID® Access Cloud Authentication Service Documentation/ [Електронний ресурс] – Режим доступу: <https://community.rsa.com/t5/rsa-securid-access-cloud/cloud-authentication-service-overview/ta-p/569175>.

АНАЛІЗ МЕТОДІВ ОЦІНКИ ПОКАЗНИКІВ ЯКОСТІ ОБСЛУГОВУВАННЯ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ

Козак А.Ю., Могилевич Д.І.

Інститут телекомунікаційних систем, КПІ ім. Ігоря Сікорського

E-mail: anastasiia.kozak18@gmail.com

ANALYSIS OF METHODS OF EVALUATION OF QUALITY INDICATORS OF MULTISERVICE NETWORK

The main methods of evaluation of service quality indicators in multiservice networks are investigated, the optimal solutions for a high level of service provision are analyzed.

Досліджено основні методи оцінки показників якості обслуговування в мультисервісних мережах, проаналізовано оптимальні рішення для високого рівня надання послуг.

Сучасна тенденція до конвергенції мереж, тобто створення універсальної мультисервісної мережі, здатної надавати послуги як комп'ютерних, так і телекомунікаційних мереж призводить до необхідності одночасного перенесення різних видів трафіку, в тому числі, чутливого до затримок. Щоб забезпечити високу якість обслуговування має існувати можливість його оцінки.

Так як кожна з цих послуг висуває свої вимоги для якісної передачі каналом зв'язку (приклад наведено в таблиці 1), то всі вони мають враховуватись при побудові мультисервісної мережі.

Таблиця 1. Вимоги до якості обслуговування для різних типів послуг.

Параметри QoS Категорія сервісу	Втрата пакетів Р, %	Пропускна спроможність С, кбіт/с	Джитер J, мс	Затримка пакетів T, мс
ІР-телефонія	0,1	64	<150	<300
Відео-конференція	0,8	2048	<30	<100
ІРTV	1,5	10240	50	500
Дані	0,1	2048	1000	1000
Відео за запитом	0,05	4096	30	1000

У рекомендації ITU Y.1540 [1,5] визначені наступні мережеві характеристики, як найбільш важливі з точки зору ступеня їх впливу на якість обслуговування (пропускна здатність, надійність мережі/мережевих елементів, затримка (мс) і джитер затримки, величина втрат (%), живучість) від одного інтерфейсу користувач-мережа User Network Interface (UNI) до іншого інтерфейсу користувач-мережа UNI).

Перераховані мережеві характеристики є необхідними для побудови моделі якості послуг в IP-орієнтованих мережах, однак будучи технічними характеристиками, вони не відображають власне якості в розумінні користувача. Для оцінювання якості надання послуг використовують показник оцінювання якості сприйняття послуг QoE (Quality of Experience), який прямо пропорційно залежить від показника якості надання сервісу QoS (Quality of Service). QoE – це суб'єктивна оцінка послуги на прикладному рівні користувачем, який користується послугою. QoS – це набір технологій мережевого та каналного рівнів, використання яких дозволяють ефективніше використовувати ресурси мережі, особливо під час передавання поточкових видів трафіку для забезпечення необхідного достатнього рівня QoE [2].

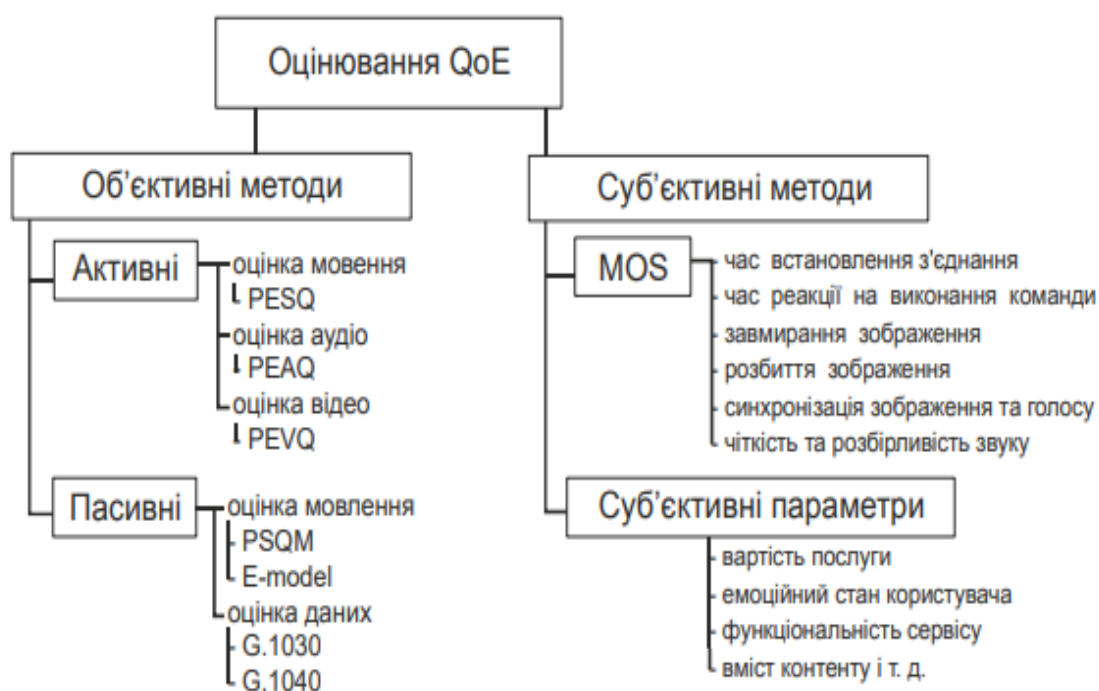


Рис.1. Загальна класифікація алгоритмів та методів оцінювання QoE.

Об'єктивні методи оцінювання якості дозволяють виключити людину із процедури оцінювання, а отже і легко автоматизуються. Об'єктивні методи поділяються на активні та пасивні. В активних методах оцінювання якості здійснюється шляхом порівняння еталонної послідовності (оригіналу) із

послідовністю, яка була викривлена під час передавання по мережі.

Найпростішим варіантом оцінки параметра QoE може слугувати оцінка MOS. Для оцінки QoE оцінюють такі параметри: час встановлення з'єднання; час реакції на виконання команди; завмирання зображення; розбиття зображення; синхронізацію зображення та голосу; чіткість та розбірливість звуку. Проте модель MOS не враховує ряд явищ, типових для пакетних мереж, що впливають на якість послуги. У моделі MOS відсутня можливість кількісно врахувати вплив факторів на якість мовлення. Важливим фактором також є те, що різний тип трафіку по-різному впливає на уявлення абонента про якість наданої послуги доступу в мережу Інтернет, і тому задача визначення та управління різних типів трафіку з позиції їх впливу на враження абонента є актуальною і пріоритетним завданням для операторів телекомунікаційних мереж [3,4,6].

Висновки. Довгий час в ролі основних методів оцінки показників якості послуг мультисервісної мережі розглядалися тільки суб'єктивні методи, проте, їх широке використання в процесі експлуатації послуг не є можливим через складність проведення тестів (необхідність постійно утримувати групи експертів). Тому останнім часом великої популярності набули методи об'єктивної оцінки, які гуртуються на зборі та аналізі мережевих характеристик.

Література

1. МСЭ-Т Recommendation Y.1540. IP Packet Transfer and Availability Performance Parameters//December 2002.
2. Є. М. Чернихівський, В. В. Червенець, О. Б. Білик. Визначення часових параметрів обслуговування потокового трафіку з пріоритетними класами // Вісник Національного університету "Львівська політехніка". – 2011. – № 705 : Радіoeлектроніка та телекомунікації. – С. 167-170.
3. ETSI, —Human Factors (HF); Quality of Experience (QoE) requirements for realtime communication services,|| European Telecommunications Standards Institute, TR 102 643, Jan. 2010.
4. M. N. Zapater and G. Bressan, —A Proposed Approach for Quality of Experience Assurance of IPTV,|| in First International Conference on the Digital Society. ICDS '07., 2007.
5. A. Takahashi, D. Hands, and V. Barriac, —Standardization activities in the ITU for a QoE assessment of IPTV,|| Communications Magazine, IEEE, vol. 46, no. 2, pp. 78 –84, february 2008.
6. K. Seshadrinathan, R. Soundararajan, A. Bovik, and L. Cormack, —Study of Subjective and Objective Quality Assessment of Video,|| Image Processing, IEEE Transactions on, vol. 19, no. 6, pp.1427 –1441, june 2010.

ДОСЛІДЖЕННЯ ПОКАЗНИКІВ ЧУТЛИВОСТІ ХАРАКТЕРИСТИК СМО З ПРІОРИТЕТАМИ ДО ЗМІН СТРУКТУРИ ОБСЛУГОВУВАННЯ

Уривський Л.О., Мартинова К.Г.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського

E-mail: scorpio.for.teen@gmail.com

THE RESEARCH OF PRIORITY QUEUEING SYSTEMS' SENSITIVITY CHARACTERISTICS TO SERVICE STRUCTURE ALTERATIONS

Sensitivity characteristics of queueing systems help to estimate and understand the systems' behavior much better. In this report, it is defined how do Sensitivity characteristics impact on the service structure.

Ототожнюючи характеристики телекомунікаційної системи і відповідної їй системи масового обслуговування (СМО), можна сформулювати рекомендації щодо раціональної побудови та організації систем передачі інформації на каналному рівні при відомій сукупності ресурсів каналів телекомунікацій [2].

Важливу роль у визначенні і оптимізації ключових показників ефективності телекомунікаційних мереж відіграють показники чутливості складних систем, які забезпечують оцінювання і додаткове розуміння поведінки системи [1].

Об'єкт дослідження – СМО з пріоритетним обслуговуванням. Розглядаються відносний та абсолютний пріоритети.

Формула (1) є аналітичною моделлю СМО з довільним числом обслуговуючих приладів(ОП) і місць для черги, але двома потоками заявок. Аналітична модель побудована за методикою, запропонованою в [2].

$$P_0 = \frac{1}{1 + \sum_n \sum_r \frac{\rho_1^{n+r}}{n! n^r} + \sum_n \sum_r \frac{\rho_2^{n+r}}{n! n^r} + \sum_n \left(\frac{\rho_2^{n+R}}{n! n^r} \cdot \frac{1}{1 + \frac{L_1}{n\mu_2}} \right) + \sum_n \left(\frac{\rho_2^{n+R}}{n! n^r} \cdot \frac{1}{1 + \frac{L_1}{n\mu_2}} \cdot \frac{L_1}{M_2} \right) + \sum_n \left(\frac{\rho_1^{n+r}}{n! n^r} + \frac{\rho_2^{n+R}}{n! n^r} \cdot \frac{1}{1 + \frac{L_1}{n\mu_2}} \cdot \frac{M_2}{n\mu_1} \right)} \quad (1)$$

При $L_1 = \lambda_1$, $M_2 \rightarrow \infty$ отримаємо систему з абсолютним пріоритетом. Система з відносним пріоритетом має відповідати таким умовам: $L_1 = \lambda_1$, $M_2 = \mu_2$. Для випадку, коли нарощується число ОП необхідно дотримуватися умов: $n = 1..N-1$; для випадку нарощування черги: $r = 0..R-1$, де N – число обслуговуючих приладів, а R – кількість місць для черги.

Вплив нарощування обслуговуючих приладів на чутливість показника продуктивності СМО. На рис. 1 зображена динаміка чутливості продуктивності 1-го і 2-го потоків для пріоритетних СМО в залежності від зміни числа обслуговуючих приладів.

Найбільш чутливим виявився 1-ий потік заявок СМО з відносним пріоритетом. Найменш чутливим виявився другий потік заявок в СМО з абсолютним пріоритетом. Відповідно, чим більший приріст числа ОП, тим гірше для продуктивності, оскільки прилади простоють [3,4].

На рис. 2 зображено динаміку чутливості показника середнього часу перебування заявки в системі від зміни числа обслуговуючих приладів. По-перше, показники потоку заявок вищого пріоритету більш чутливі до нарощування обслуговуючих приладів. По-друге, в досліджуваних СМО заявки або обслуговуються, або втрачаються, або очікують обслуговування.

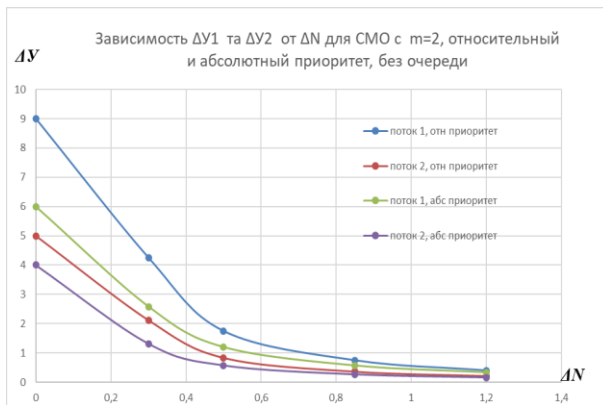


Рис. 1. Залежність чутливості показника продуктивності пріоритетних СМО в залежності від зміни числа обслуговуючих приладів.

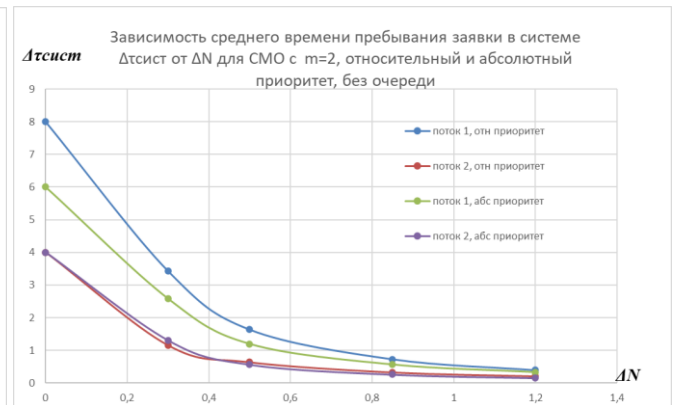


Рис. 2. Залежність чутливості показника середнього часу перебування заявки в системі пріоритетних СМО в залежності від зміни числа обслуговуючих приладів.

Відтак, при постійному вхідному навантаженні заявки і при зростаючому приросту ОП, середня тривалість перебування заявки в системі $\tau_{\text{сист}}$ знижується. Дана обставина є безперечно вигідною для користувача послугами. Варто зауважити, що криві показника $\tau_{\text{сист}}$ для потоків заявок другого типу мають точку перетину при $\Delta N=0,4$. Дана обставина є передумовою для подальшого дослідження показника середнього часу перебування заявки в системі ($\tau_{\text{сист}}$) в контексті ситуаційного керування.

Підсумовуючи розглянуті графіки, сформулюємо наступний висновок: зміна числа обслуговуючих приладів є інструментом для ситуаційного керування. Більш того, потоки заявок вищого пріоритету більш чутливі до нарощування приладів.

Вплив нарощування черги на чутливість показника продуктивності СМО. Розглянемо вплив нарощування черги на показники чутливості характеристик QoS. На рис.3 очевидно, що потоки заявок нижчого пріоритету більш чутливі до нарощування черги, особливо СМО з відносним пріоритетом. При збільшенні числа місць для черги до 30%, спостерігається найбільша різниця значень показника чутливості для потоків заявок першого типу – 0,5.

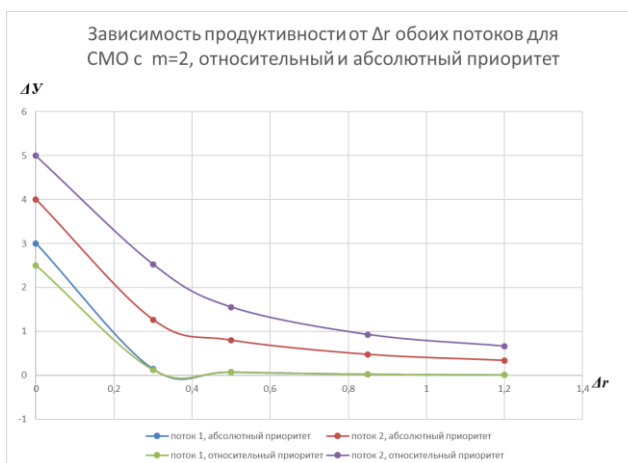


Рис. 3. Залежність чутливості продуктивності пріоритетних СМО в залежності від зміни числа місць для черги.

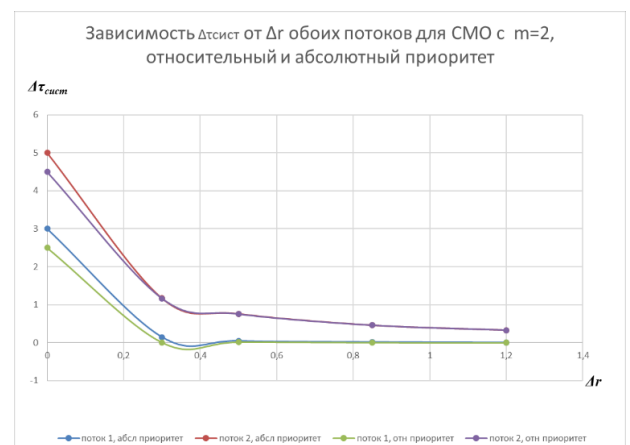


Рис. 4. Залежність чутливості показника середнього часу перебування заявки в системі пріоритетних СМО в залежності від зміни числа місць для черги.

На рис. 4 зображено динаміку чутливості показника середнього часу перебування заявки в системі в залежності від зміни числа місць для черги.

Досліджуючи СМО з чергою важливо проаналізувати показник середнього числа заявок в черзі, в даній статті – чутливість показника середнього числа місць для черги (рис.5). Очевидно, що потоки заявок другого типу мають вищу чутливість до нарощування черги, ніж потоки заявок першого типу. Різниця значень чутливості $\Delta r_{очер}$ мала, проте досягає максимуму при $0,2 \leq \Delta r \leq 0,5$. Відзначимо, що графік має асимптотичний характер.

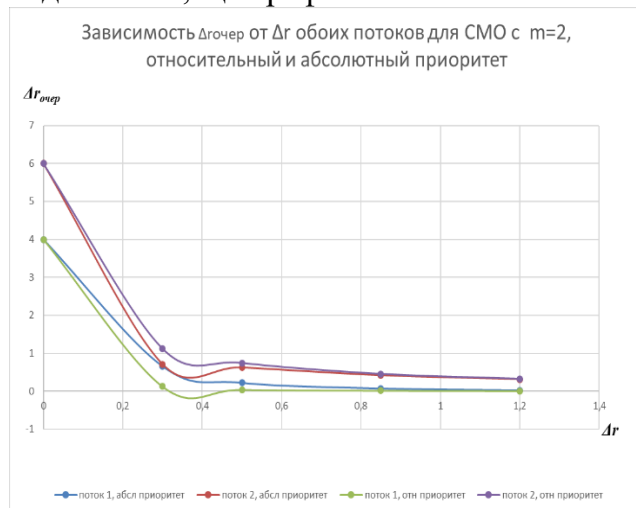


Рис. 5. Залежність чутливості показника середнього числа заявок в черзі пріоритетних СМО в залежності від зміни числа місць для черги.

Висновки. Підсумуємо отримані результати: зміна числа місць для черги значно підвищує чутливість показників QoS заявок нижчого пріоритету.

Отже, отримано комплексну аналітичну модель для пріоритетних СМО з довільним числом ОП, чергою довільної довжини, але двома потоками заявок [2]. Зокрема розглянуто відносний та абсолютний пріоритети.

Визначено, що зміна числа обслуговуючих приладів є інструментом для ситуаційного керування. Крім того, з'ясовано, що потоки заявок вищого пріоритету більш чутливі до нарощування приладів. Також визначено, що зміна числа місць для черги значно підвищує чутливість показників QoS заявок нижчого пріоритету.

Література

1. Торошанко Я.І. Управление надёжностью телекоммуникационной сети на основе анализа чувствительности сложных систем / Я. І. Торошанко // Телекоммуникаційні та інформаційні технології. – 2016. – № 3. – С. 31–36.
2. Uryvsky L., Martynova K. Complex analytical model of priority requires service on cloud server / 2019 International Conference Radio Electronics & Info Communications (UkrMiCo). – IEEE Xplore Digital Library. – <https://ieeexplore.ieee.org/document/9165323>.
3. Уривський Л.О., Гахова А.С. Сценарій реалізації ситуаційних пріоритетів обслуговування в системах доступу / К.: ІТС КПІ ім. Ігоря Сікорського, XI Міжнародна НТК «Проблеми телекомунікацій», /Збірник матеріалів. – 2017, с. 66...68.
4. Martynova K.G. Scopes to solve the task of telecommunication resources distribution to provide the required QoS. /XIV Міжнародна науково-технічна конференція «Перспективи телекомунікацій» ПТ-2020: Збірник матеріалів конференції К.: КПІ ім. Ігоря Сікорського. – 2020. – с.352-354.

ВИЗНАЧЕННЯ ЗАВАДОСТІЙКОСТІ СКК В УМОВАХ НИЗЬКОЇ ЕНЕРГЕТИКИ

Уривський Л.О., Шмігель Б.О.

Інститут телекомунікаційних систем КІП ім. Ігоря Сікорського, Україна

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

NOISE IMMUNITY EVALUATION FOR SIGNAL CONSTELLATION IN LOW ENERGY CONDITIONS

In this paper considered a comparative analysis of the noise immunity of signal constellation. The properties signals in low energy conditions are analyzed.

За останні десятиліття цифрові комунікації вступили в фазу бурхливого розвитку, яка активно продовжується і в теперішній час. На сьогоднішній день безпроводові широкосмугові мережі набули швидкого розповсюдження. Використання сигнально-кодових конструкцій (СКК) дозволяє найбільш ефективно використовувати ресурси каналу, адже одночасно можливо отримати вииграш як з енергетичної, так частотної ефективності або, у всякому разі, отримати вииграш по одному показнику, не погіршуючи інший.

Тим самим, використовуючи оптимальні комбінації СКК, досягається найкраща інформаційна ефективність – відношення пропускної здатності до продуктивності при обмежених ресурсах каналу зв'язку, і одночасно задовольняються вимоги до необхідного рівня достовірності інформації.

Правильний підбір комбінації СКК дозволить мінімізувати втрати в заданій зоні покриття, оптимізувати значення потужностей передавачів, пропускну здатність і стійкість системи.

В технічній літературі приводяться різні співвідношення для розрахунку ймовірності помилки маніпульованого символу багатопозиційним сигналом ($P_{\text{сим}}$) і помилки інформаційного символу, тобто біту ($P_{\text{біт}}$) [1 - 4]. До тих результатів, які викликають найбільшу довіру, слід віднести результати векторно-фазового методу [2], та результати за Дж. Прокісом [1].

Завдання полягає в тім, щоб отримати більш точні аналітичні співвідношення для визначення ймовірностей помилок для більш широкого набору маніпуляцій.

В доповіді проведено аналіз згідно набору маніпуляцій: BPSK, QPSK, QAM-16 (Quadrature Amplitude Modulation), QAM-64 – які аналітично розраховані та графічно побудовані за допомогою формул Дж. Прокіса [1].

Графіки дослідження символної помилки та відношення сигнал/шум для кожної модуляції розраховані та побудовані в програмі Matlab мають

наступний вигляд (рис.1):

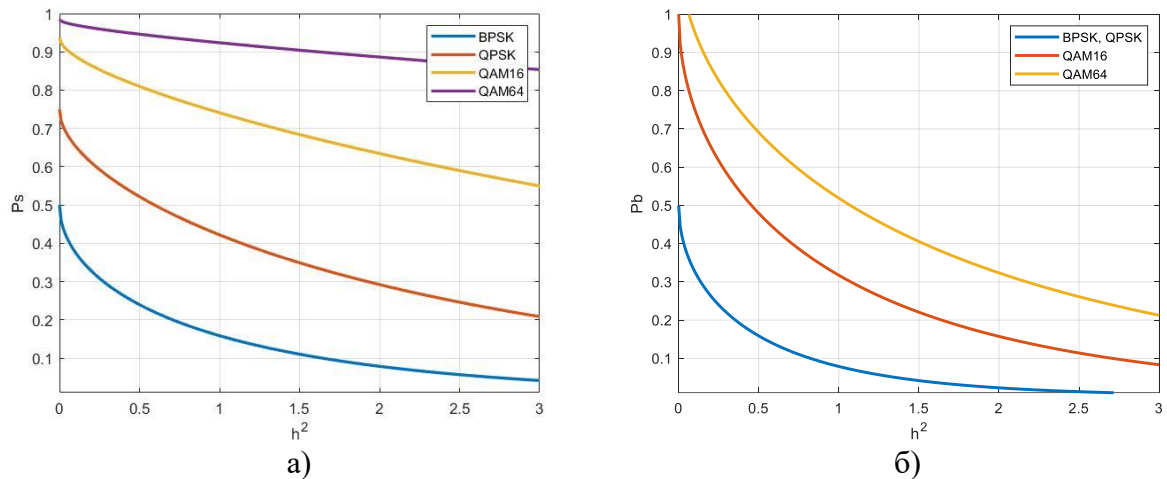


Рис. 1. Графік залежності ймовірності помилок (а – помилка передачі символу, б – бітова помилка) від h^2 для BPSK, QPSK, QAM-16, QAM-64.

З рисунку 1 (зокрема, з рис.1б) видно, що в умовах низької енергетики ($h^2 < 3$) формули Прокіса не є точними ($P_b > 0,5$). Це пояснюється тим, що аналітичні формули враховують лише попадання результуючого вектору сигналу сусідню область, однак не враховує попадання вектору в більш віддалені області.

Для отримання точних результатів пропонується використовувати векторно-фазовий метод, в основі якого лежить визначення ймовірності попадання результуючого (сумарного) вектору сигналу й перешкоди в деяку просторово-фазову область, в якій перешкода призводить до неправильного приймання символів багатократної маніпуляції [2]. Нехай в канал зв'язку передається сигнал S (рис.2). Під впливом перешкоди W сигнал S утворює результуючий сигнал r , який приходить на приймач. Якщо результуючий сигнал потрапляє в область реєстрації сигналу, що передається, то сигнал приймається вірно, якщо ж результуючий сигнал знаходиться поза області достовірної реєстрації сигналу, що передається, то він приймається невірно.



Рис. 2. Векторне представлення впливу перешкоди на результуючий сигнал.

Варто зауважити, що символна помилка використовується як проміжний етап при розрахунку бітової помилки. Важливим показником стану каналу зв'язку є бітова помилка, однак розрахунки бітової помилки для низької енергетики не є точними. Для невеликих значень відношення сигнал/шум значення бітової помилки розходяться, але при збільшенні h^2 це розходження становиться менш помітним. Векторно-фазовий метод дає змогу отримати точні розрахунки при будь-якій енергетиці, на відміну від формул Прокіса, що можуть використовуватись тільки для високої енергетики каналу.

Особливість формул за векторно-фазовим методом полягає у їх достовірності, адже вони більш точно вираховують ймовірності помилок та не піддаються такої ж універсалізації як інші формули розрахунку ймовірності символних і бітових помилок.

Висновки. Ефективність використання ресурсів каналу описує показник інформаційної ефективності, який являє собою відношення продуктивності до пропускну здатності каналу зв'язку. Для досягнення високого показника інформаційної ефективності необхідно оперувати оптимальним вибором сигнально-кодових конструкцій.

Розраховано та порівняно значення ймовірностей символної та бітової помилок в умовах низької енергетики за векторно-фазовим методом та допомогою формул Дж. Прокіса.

Важливим показником стану каналу зв'язку є бітова помилка, однак розрахунки бітової помилки для низької енергетики не є точними. Для невеликих значень відношення сигнал/шум значення бітової помилки розходяться з результатами розрахунків за універсальними формулами [1], але при збільшенні відношення сигнал/шум це розходження становиться менш помітним. Векторно-фазовий метод дозволяє отримати точні розрахунки при будь-якій енергетиці, на відміну від формул Прокіса, що можуть використовуватись тільки для високої енергетики.

Особливість формул за векторно-фазовим методом полягає у їх достовірності, адже вони більш точно вираховують ймовірності помилок, але не піддаються такої ж універсалізації, як інші формули розрахунку ймовірності символних і бітових помилок.

Література

1. Прокіс, Дж. Цифровая связь / Пер. с англ.; Под ред. Д.Д. Кловского - М.: Радио и связь, 2000. – 800 с.
2. Урывский Л. А., Прокопенко Е. А., Наталенко А. И. Векторно-фазовый метод для определения показателей помехоустойчивости многопозиционных сигналов. – Зв'язок, № 12, 2012. – с. 58-63.
3. Sklar B, Digital communications: Fundamentals and Applications. — 2nd Edition – University of California, Los Angeles, 2001. – 1004 p.
4. Феер К. Беспроводная цифровая связь: методы модуляции. / Пер. с англ. под ред. В. И. Журавлёва. — М.: Радио и связь, 2000. — 520 с.

ПОБУДОВА КОМП'ЮТЕРНИХ КЛАСТЕРІВ ДЛЯ МОДЕЛЮВАННЯ НАДСКЛАДНИХ ПРОЦЕСІВ У ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ НА БАЗІ ОПЕРАЦІЙНОЇ СИСТЕМИ LINUX

Вакуленко О.В., Кирилова В.Д.

Інститут телекомунікаційних систем КІП ім. Ігоря Сікорського, Україна

E-mail: kirilova_vika2000@icloud.com

CONSTRUCTION OF COMPUTER CLUSTERS FOR MODELING COMPLEX PROCESSES IN TELECOMMUNICATION SYSTEMS BASED ON LINUX OPERATING SYSTEM

The main approaches to the construction of computer clusters for modeling complex processes in telecommunication systems are considered based on Linux operating system for educational institutions.

Проблемам побудови комп'ютерних кластерів для моделювання надскладних процесів у телекомунікаційних системах на базі операційної системи Linux присвячено останніми роками багато уваги [1÷8]. Одним з напрямів, являється організація кластерів на базі вже існуючих мереж робочих станцій, тобто робочі станції можуть використовуватися в якості вузлів кластера вночі та в неробочі дні. Системи такого типу називають COW (Cluster of Workstations). В цьому випадку реальним видається варіант, коли кластер будується на основі існуючого комп'ютерного класу та окремих робочих станцій закладу вищої освіти. Під час навчального процесу виникають задачі пов'язані з проведенням моделювання надскладних процесів у телекомунікаційних системах для яких продуктивність одного комп'ютера недостатньо. Тому побудова і застосування комп'ютерних кластерів на базі робочих станцій закладу вищої освіти являється актуальним в наш час.

Новизна роботи визначена в комплексному підході щодо побудови комп'ютерних кластерів для моделювання надскладних процесів у телекомунікаційних системах на базі операційної системи Linux.

Практична цінність дослідження у використуванні результатів під час навчального процесу для проведення наукових досліджень шляхом моделювання надскладних процесів у телекомунікаційних системах на базі

комп'ютерних кластерів побудованих на робочих станціях закладу вищої освіти.

Метою дослідження є підвищення ефективності навчального процесу при проведенні досліджень шляхом моделювання надскладних процесів у телекомунікаційних системах на базі комп'ютерних кластерів під управлінням операційної системи Linux.

Об'єкти дослідження це процеси функціонування комп'ютерних кластерів під управлінням операційної системи Linux.

Предметом дослідження є методики побудови комп'ютерних кластерів для моделювання надскладних процесів у телекомунікаційних системах на базі операційної системи Linux.

Вихідні дані:

Дано: робочі станції закладу вищої освіти; програмне забезпечення для ОС Linux.

Обмеження: застосовується програмне забезпечення, яке знаходиться у вільному доступі, операційна система робочих станцій – Linux.

Необхідно: розробити алгоритм побудови та застосування комп'ютерних кластерів для моделювання надскладних процесів у телекомунікаційних системах на базі операційної системи Linux.

Етапи побудови комп'ютерного кластеру:

- Встановити операційну систему на комп'ютер, який буде виступати в ролі консолі кластера.
- Встановити компілятори (фортран, С) і всі необхідні бібліотеки, desktop environment (GNOME або KDE), текстові редактори та ін., тобто перетворити цей комп'ютер в робочу станцію розробника.
- Встановити зі сховищ або з початкових кодів пакет MPICH або OpenMPI, якщо він Вам більше до душі.
- Описати в / etc / hosts майбутні вузли вашого кластера, в тому числі і консоль кластера.
- Встановити NFS і надати доступ для всіх вузлів кластера директорію, в якій будуть розміщуватися виконувані модулі паралельних програм та файли даних, якими ці програми будуть користуватися в процесі своєї роботи.
- Встановити на консолі кластера ssh-клієнт та ssh-сервер.

- На всіх вузлах кластера встановити операційну систему, бібліотеки, які необхідні для виконання призначених для користувача паралельних програм. Встановити MPICH, NFS-client, ssh-server. Вузли кластера з метою економії ресурсів повинні завантажуватися в runlevel 3.
- Описати в / etc / hosts всіх вузлів кластера майбутні вузли вашого кластера, в тому числі і консоль кластера.
- На всіх вузлах кластера встановити при завантаженні монтування відкритого ресурсу консолі кластеру. Шлях до цього ресурсу повинен бути однаковий, як на консолі кластера, так і на його вузлах. При умові надання загального доступу до каталогу / home / mpiuser / data, а також, на вузлах кластера, цей ресурс повинен бути змонтований в / home / mpiuser / data.
- На всіх вузлах кластера забезпечити безпарольного доступ по ssh для консолі кластера.
- Провести оптимізацію комп'ютерного кластеру.

Висновки. Отже в роботі розглянуто методики побудови комп'ютерних кластерів для моделювання надскладних процесів у телекомунікаційних системах на базі операційної системи Linux. Завдяки яким підвищиться ефективність навчального процесу при проведенні досліджень шляхом моделювання надскладних процесів у телекомунікаційних системах на базі комп'ютерних кластерів під управлінням операційної системи Linux.

Література

1. Воеводин Вл.В., Жуматий С.А. Вычислительное дело и кластерные системы: Монография. - М.: Изд-во МГУ, 2007. - 150 с.
2. Баденко В.Л. Высокопроизводительные вычисления: Учебное пособие. - СПб.: Изд-во Политехн. ун-та, 2010. - 180 с.
3. Лупин С.А., Посыпкин М.А. Технологии параллельного программирования. М.: ИД «ФОРУМ»: ИНФРА-М, 2011. — 208 с.
4. Антонов А.С. Параллельное программирование с использованием технологии MPI. : Учебное пособие. – М.: Изд-во МГУ, 2004. – 71 с. ISBN 5-211-04907-1.
5. Гергель В.П. Высокопроизводительные вычисления для многоядерных многопроцессорных систем: Учебное пособие. – Ниж.Н.; Изд-во ННГУ им. Н.И. Лобачевского, 2010. - 420 с..
6. Сайт <http://www.parallel.ru>.
7. Сайт <http://cluster.linux-ckb.info>.
8. Сайт <http://iproc.ru/programming/mpich-wind>.

УДОСКОНАЛЕНА МЕТОДИКА СИНТЕЗУ АЛГОРИТМІВ ВИЯВЛЕННЯ-РОЗДІЛЕННЯ ВЗАЄМНО НЕОРТОГОНАЛЬНИХ СИГНАЛІВ ПРИ ПАКЕТНОМУ РЕЖИМІ ПЕРЕДАЧІ

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: tzadikalex@gmail.com

THE IMPROVED METHOD OF SYNTHESIS OF ALGORITHMS OF EXPOSURE-DIVISION MUTUALLY OF UNORTOGONAL SIGNALS IS AT BATCH MODE OF TRANSMISSION

The technique of synthesis of detection-separation algorithms which realizes a problem of the decision of pair conflicts at a packet mode of transfer in systems of multiuser access is offered.

Проблемі повторного використання частотного ресурсу приділяється багаторічна невпинна увага [1, 2]. Фундаментом теоретичних досліджень в зазначеній галузі є так звана теорія багатокористувацького детектування – БКД (Multiuser detection theory – MDT [4, 5]) і її відгалуження – статистична теорія розділення цифрових сигналів – СТРС [1, 2]. Актуальність розглянутої роботи зумовлена в першу чергу проблемами багатокористувацького доступу. Справді, в системах зв'язку, в яких деяка більшість джерел двійкової інформації не відображена в праві роботи будь-якого з них на передачу в довільний момент часу, можливі конфлікти – одночасний вихід на передачу більш ніж одного користувача. Донедавна передбачалось, що при виникненні будь-якого такого конфлікту, всі заявки, що зіткнуться – помирають, якщо тільки не відбувається так названого «захоплення» однієї, найбільш потужної з них. Змістовно явище «захоплення» проаналізовано в [1]. Варто зауважити при цьому [2], що для забезпечення можливості «захоплення» необхідне виконання двох вимог: а) введення обов'язкового розподілу користувачів хоча б на дві групи, достатньо розділених за потужністю, для реалізації такого «захоплення» (який можна назвати кореляційним поділом); б) забезпечення факту виходу на передачу тільки одного користувача з групи із більшою потужністю.

Враховуючи, що в практично найдоцільніших системах багатокористувацького доступу з однаковими інтенсивностями кожного з користувачів найбільш ймовірні парні зіткнення, тому розробка методики синтезу алгоритмів виявлення-розділення, яка реалізує задачу вирішення парних конфліктів при пакетному режимі передачі, являється актуальною в наш час.

Новизна роботи визначена в комплексному підході щодо підвищення завадостійкості виявлення-розділення взаємно неортогональних цифрових сигналів при пакетному режимі передачі.

Практична цінність. Результати дослідження доцільно використовувати при розробці систем багатокористувацького доступу, які здійснюють вирішення задачі парних конфліктів при пакетному режимі передачі.

Мета дослідження. Підвищення завадостійкості виявлення-розділення взаємно

неортогональних цифрових сигналів.

Об'єкт дослідження. Процеси функціонування цифрових радіоліній з випадковим множинним доступом.

Предмет дослідження. Методики синтезу алгоритмів виявлення-розділення взаємно неортогональних цифрових сигналів при пакетному режимі передачі.

Вихідні дані:

Дано: канал з постійними параметрами АБГШ; всі неінформаційні параметри сигналів відомі; сигнали взаємно неортогональні з пакетним режимом передачі.

Обмеження: $S_1(t)$ відрізняється від $S_2(t)$ не менш ніж на 6 дБ; аналіз здійснюється на інтервалі передачі одного пакету.

Необхідно: розробити методику синтезу алгоритмів виявлення-розділення взаємно неортогональних сигналів при пакетному режимі передачі на основі критерію мінімуму імовірності помилки ($\min P_{\text{пом}}$).

Етапи реалізації методики:

1. Формування моделі спостереження трійкових сигналів.

Модель спостереження допускає, що мають місце зіткнення пари сигналів користувачів з двох різних за потужністю груп, представлено у вигляді:

$$y_1 = \left[(-1)^{r_1} + r_1 (1 - r_1) / 2 \right] S_1(t) + \left[(-1)^{r_2} + r_2 (1 - r_2) / 2 \right] S_2(t) + n(t) \quad (1)$$

$$t \in [t_{k-1}, t_k]; k = 1, 2, \dots; r_i = 0, 1, 2; i = 1, 2,$$

тут $S_1(t)$ і $S_2(t)$ – відомі інтегруючі в квадраті функції, які характеризують у загальному випадку широкосмугові псевдовипадкові переривчасті сигнали (ПС) без інформаційної маніпуляції; $r_1, r_2 \in \{0, 1, 2\}$ – дискретні інформаційні параметри сигналів; при цьому згідно (1) стан $r_1, r_2 = 2$ відповідає відсутності випромінювання ПС; $n(t)$ – адитивний білий гаусівський шум (АБГШ); t_k – моменти прийняття рішення зміни (тактової точки) стану дискретних параметрів (ДП); $r_1 : r_2 : k_1$ – номер інформаційного тактового інтервалу.

2. Введення апіорних імовірностей для визначення апостеріорних на весь інтервал спостереження.

На основі байєсівського підходу проводиться формування апіорних імовірностей для подальшого визначення апостеріорних на весь інтервал спостереження.

3. Одержання апостеріорних ймовірностей в явному виді.

Формуються апостеріорні імовірності в явному виді на підставі станів, які можуть приймати цифрові сигнали при пакетному режимі.

4. Конструювання правил прийняття рішення.

Правило прийняття рішення формується за критерієм максимуму апостеріорної ймовірності [2] та записується в еквівалентній формі використовуючи вирішальну функцію Хевісайда:

$$r_i^* = \text{rect} [P(r_i = 1 / y_i) - P(r_i = 0 / y_i)] (1 - Q_i); \quad r_i^* = \overline{0, 1};$$
$$Q_i = \text{rect} [P(r_i = 2 / y_i) - P(r_i = 0 / y_i)] \cdot \text{rect} [P(r_i = 2 / y_i) - P(r_i = 1 / y_i)]; \quad Q_i = \overline{0, 1}. \quad (2)$$

5. Синтез структурної схеми виявлення-розділення взаємно неортогональних сигналів при пакетному режимі передачі.

На основі алгоритму виявлення-розділення взаємно неортогональних сигналів при пакетному режимі синтезуємо структурну схему, яка представлена на рис. 1.

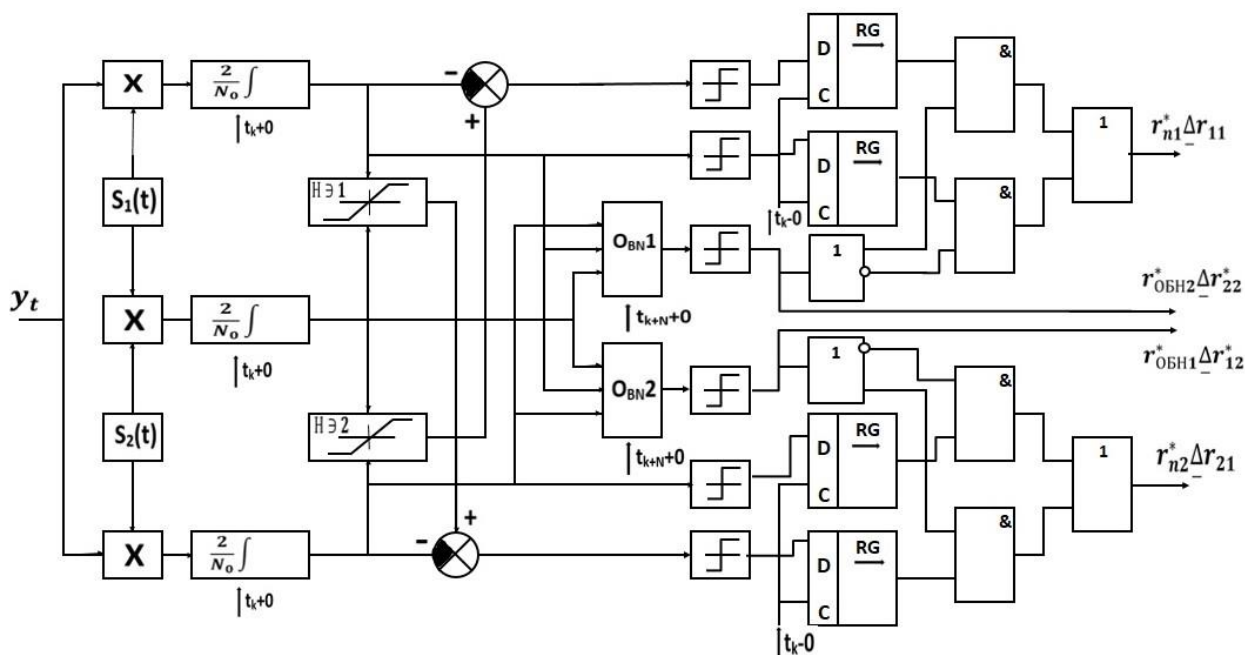


Рис. 1. Структурна схема демодулятора з розв'язанням парних конфліктів між інформаційними ФМ-пакетами.

6. Перевірка роботоспроможності схеми.

Перевірка роботоспроможності здійснюється на основі виведених правил прийняття рішень (2) по критерію $\min P_{\text{пом}}$.

Висновки. Запропонована методика синтезу алгоритмів виявлення-розділення взаємно неортогональних цифрових сигналів при пакетному режимі передачі дозволяє підвищити завадостійкість виявлення-розділення взаємно неортогональних ЦС завдяки, в порівнянні з одиночними ЦС, більшій енергетики пакету ЦС.

Література

1. Бураченко Д.Л. Оптимальное разделение цифровых сигналов многих пользователей в линиях и сетях связи в условиях помех. Ленинград: ВАС, 1990, 302 с.
2. Ерохин В.Ф. Багатокористувачке детектування: навчальний посібник / К.: ІСЗІ КПІ ім. Ігоря Сікорського, 2017. 162 с.
3. Колмогоров А.Н. Об оценке параметров стационарного гауссовского марковского процесса. ДАН СССР, 1962, Т.146, с. 747-750.
4. Duel-Hallen A.A family of multiuser decision-feedback detectors for asynchronous CDMA channels. IEEE Transactions on Communications, 1995, №43 (2/3/4), p.p. 421-434.
5. Lupas R., Verdu S. Linear Multiuser Detectors for Synchronous Code – Division Multi-Access Channels. IEEE Trans on Inf. Theory. Vol 35, №1, January, 1989, p.p. 123-136.
6. Sh. Moshavi. Multi-user Detection for DS-CDMA Communications // Bellcore pub., Oct. 1996. IEEE Communications Magazine, 23 p.
7. Verdu S. Multiuser detection. Cambridge: Cambridge university Press, 1998, 474 p.
8. Verdu S. Minimum probability of error for synchronous Gaussian multiple-access channels/ IEEE Transactions Information Theory, 1986, №32, p.p. 85-96.

МЕТОДИКА ВИЗНАЧЕННЯ ПАРАМЕТРУ ШВИДКОСТІ КОДУВАННЯ ЗА АЛГОРИТМОМ УПРАВЛІННЯ СИТУАЦІЄЮ В КАНАЛІ ЗВ'ЯЗКУ ПРИ НЕЗМІННОСТІ ПРОДУКТИВНОСТІ ДЖЕРЕЛА ПОВІДОМЛЕНЬ

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

METHODS OF DETERMINING THE CODING RATE

The main tools of the investigated algorithm are generalized. The presented tools and their interrelationships in the context of the algorithm are considered to form a technique for finding the coding rate, avoiding the procedure for finding it by the iteration method.

Сучасні системи електронних комунікацій мають напрямок розвитку у бік збільшення швидкості передачі інформації. Але збільшення швидкості потребує використання додаткових ресурсів каналу зв'язку та інструментів підтримання заданої достовірності передачі при обмежених умовах. Таким інструментом є сформований алгоритм пошуку оптимального за обсягом використаних ресурсів завадостійкого коду.

При формуванні даного алгоритму вирішується задача знаходження таких параметрів телекомунікаційної мережі, які забезпечать незмінну, сталу продуктивність джерела повідомлень при використанні додаткового частотного ресурсу (збільшення каналної швидкості передачі інформації).

В даному випадку алгоритм передбачає збільшення використання частотного ресурсу, оскільки частина ресурсу буде відокремлюватися на інструменти забезпечення достовірної передачі інформації, а саме на кодування [1, 2]. Він складається з трьох етапів (рис. 1).

На першому етапі визначаються вихідні дані для майбутнього коду – співвідношення між початковою та потрібною достовірністю передавання інформації в каналі зв'язку.

Другий етап цього алгоритму передбачає знаходження потрібної виправної здатності коду за допомогою методики, викладеної в [3]. Складність полягає в тому, що заздалегідь невідомо, який вплив матимуть дані параметри коду на фінальну продуктивність каналу зв'язку при сталій продуктивності джерела, тому необхідно перебирати різні варіанти та дивитися на результуючу продуктивність каналу. Саме через це була розроблена методика визначення параметру швидкості коду, в результаті якої можна було б одразу отримати значення швидкості кодування, яке забезпечить умову незмінності продуктивності джерела повідомлень.

Третій етап алгоритму описує останню фазу, яка забезпечує не приблизне, а точне значення потрібної продуктивності джерела. При цьому незначні уточнюючі зміни швидкості в каналі не впливають на інші параметри системи передачі.

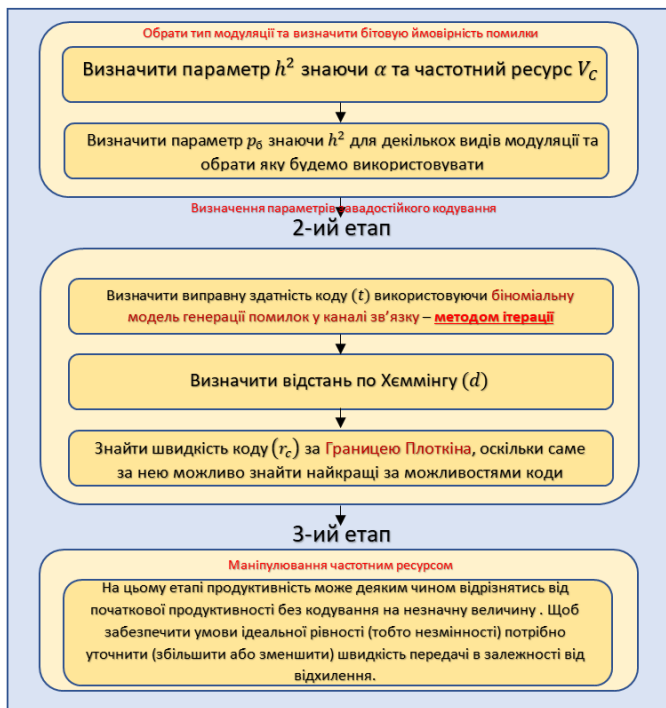


Рис. 1. Алгоритм управління ситуацією у каналі зв'язку.

Ідея запропонованої методики полягає у встановленні взаємозв'язків між початковою швидкістю кодування (початковий стан системи) системи передачі інформації та швидкістю кодування, яке забезпечить умову незмінності продуктивності джерела повідомлень (майбутній стан системи при збільшенні каналної швидкості передачі інформації).

На рис. 2 графічно представлена ідея, що полягає у пошуку взаємозв'язків між швидкістю кодування ($r_{c0(x)}$) у перетинах

початкового стану функціонування системи передачі інформації (канална швидкість передачі – $V_{c0(x)}$) та швидкістю кодування ($r_{c1(x)}$) у перетинах майбутнього стану функціонування системи передачі (канална швидкість передачі – $V_{c1(x)}$). Майбутній стан системи передачі характеризується рівністю швидкості передавання бітів джерела повідомлень із продуктивністю каналу (з урахуванням надлишковості потоку бітів в майбутньому стані системи за рахунок корегуючих кодових бітів).

Для дослідження залежностей знайдемо усі параметри даних характерних перетинів та занесемо до відповідних таблиць.

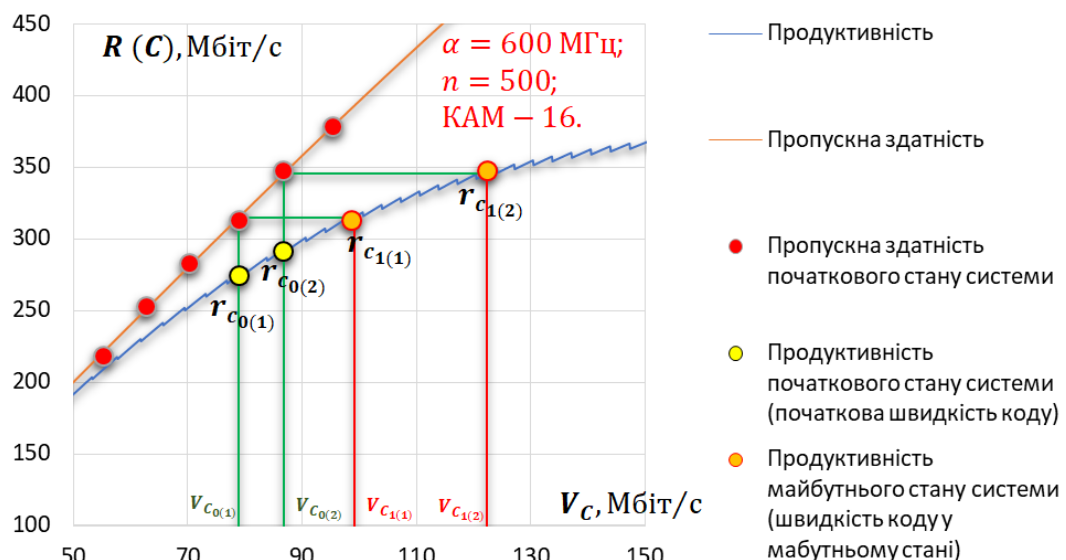


Рис. 2. Графічне представлення ідеї взаємозв'язку параметрів.

Таблиця 1. Показники параметрів системи передачі у перетинах які вважаються початковими станами системи передачі інформації

V_c , мбіт/с	h^2 , дБ	$p_{\text{біт}}$	$p_{\text{сим}}$	t	$r_{c_0(x)}$	R , мбіт/с	C , мбіт/с
15	16,02	$5,781 \cdot 10^{-9}$	$1,887 \cdot 10^{-15}$	0	1	59,99999	60
22,99	14,17	$1,835 \cdot 10^{-6}$	$1,55 \cdot 10^{-10}$	0	1	91,957	91,96
30,98	12,87	$3,104 \cdot 10^{-5}$	$3,895 \cdot 10^{-8}$	1	0,995	123,259	123,92
38,97	11,87	$1,683 \cdot 10^{-4}$	$1,04 \cdot 10^{-6}$	3	0,982	152,654	155,879
46,96	11,06	$5,206 \cdot 10^{-4}$	$9,215 \cdot 10^{-6}$	4	0,974	181,843	187,83
54,95	10,38	$1,170 \cdot 10^{-3}$	$4,377 \cdot 10^{-5}$	6	0,959	208,116	219,752
62,94	9,79	$2,157 \cdot 10^{-3}$	$1,411 \cdot 10^{-4}$	8	0,944	232,425	251,599
70,93	9,27	$3,482 \cdot 10^{-3}$	$3,513 \cdot 10^{-4}$	10	0,929	254,701	283,3
78,92	8,81	$5,121 \cdot 10^{-3}$	$7,307 \cdot 10^{-4}$	12	0,913	274,948	314,771
86,91	8,39	$7,038 \cdot 10^{-3}$	$1,333 \cdot 10^{-3}$	14	0,898	293,218	345,914
94,9	8,01	$9,192 \cdot 10^{-3}$	$2,205 \cdot 10^{-3}$	17	0,874	306,849	376,634

Таблиця 2. Показники параметрів системи передачі у перетинах які вважаються майбутніми станами системи передачі інформації

V_c , мбіт/с	h^2 , дБ	$p_{\text{біт}}$	$p_{\text{сим}}$	t	$r_{c_1(x)}$	R , мбіт/с	C , мбіт/с
15	16,02	5,781E-09	1,887E-15	0	1	59,9999996	60,00001
22,99	14,17	1,836E-06	1,551E-10	0	1	91,96	91,963
31,15	12,85	3,243E-05	4,243E-08	1	0,995	123,92	124,587
39,81	11,78	1,933E-04	1,360E-06	3	0,982	155,879	159,221
48,95	10,88	6,522E-04	1,423E-05	5	0,967	187,830	195,777
58,72	10,09	1,594E-03	7,908E-05	7	0,952	219,752	234,808
69,96	9,33	3,304E-03	3,179E-04	10	0,929	251,599	279,464
82,56	8,61	5,963E-03	9,747E-04	13	0,906	283,3	329,011
99,1	7,82	1,040E-02	2,783E-03	18	0,866	314,771	392,57
122,43	6,9	1,789E-02	7,660E-03	25	0,811	345,914	478,114
186,7	5,07	4,082E-02	3,503E-02	43	0,669	376,634	680,359

Для наочності, по отриманим даним в таблицях, варто побудувати залежність швидкості кодування в майбутньому стані системи передачі інформації ($r_{c_1(x)}$) від швидкості кодування у початковому стані системи передачі інформації ($r_{c_0(x)}$). Одразу по отриманому графіку зробимо апроксимацію для отримання формули. За допомогою неї, знаючи швидкість кодування в початковому стані системи, можливо одразу знайти швидкість кодування, яка забезпечить умову незмінності продуктивності джерела повідомлень.

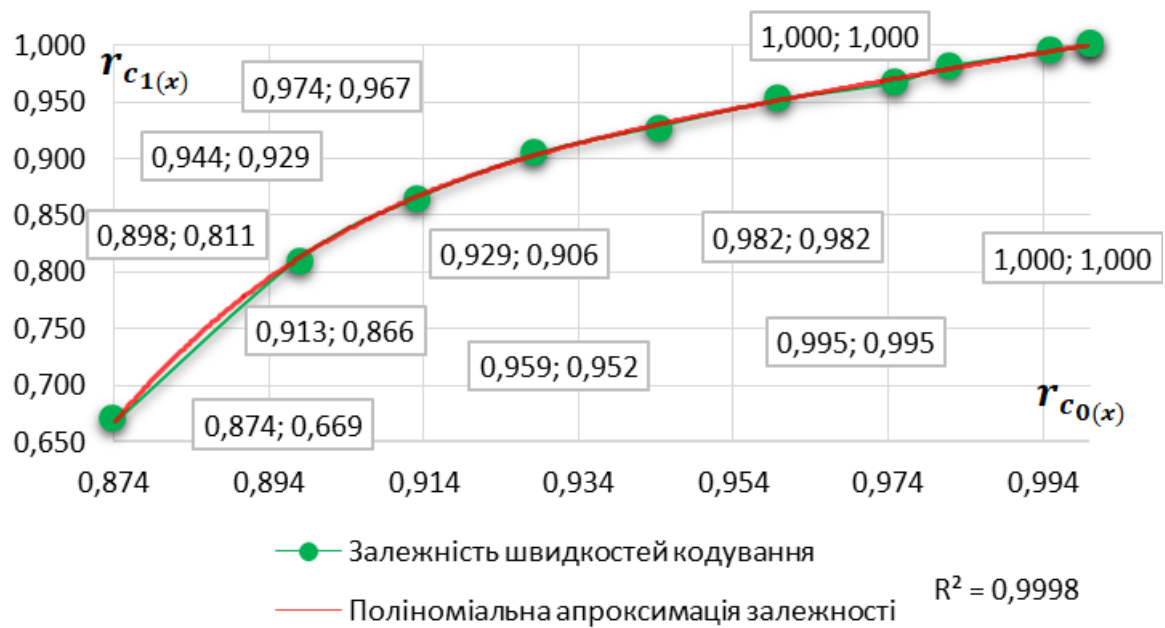


Рис. 3. Взаємозв'язок параметру швидкості кодування при двох різних станах системи.

Формула апроксимації є поліномом четвертого порядку:

$$r_{c1(x)} = -1705,5 \cdot (r_{c0(x)})^4 + 6639,4 \cdot (r_{c0(x)})^3 - 9693,9 \cdot (r_{c0(x)})^2 + 6292,6 \cdot r_{c0(x)} - 1531,6$$

Отже, в ході дослідження сформована методика визначення швидкості кодування для забезпечення заданої достовірності передачі інформації (ймовірність помилки на виході пристрою одержувача на рівні 10^{-6}) при умові незмінності продуктивності джерела повідомлень для коду довжиною блоку $n = 500$.

Результатом дослідження є представлений поліном четвертого порядку, за допомогою якого можна знайти необхідний параметр швидкості кодування при визначених вище обмеженнях.

Подальші дослідження будуть спрямовані на більш розширене число досліджуваних кодів за параметром довжини блоку коду та встановленням взаємозв'язків з іншими параметрами системи передачі інформації.

Література

1. Питерсон У. Коды, исправляющие ошибки [Текст] / У. Питерсон, Э. Уэлдон. // М.: «МИР», 1976. – 594 с.
2. Основы теории телекоммуникаций / Підручник / За заг. ред. проф. Ільченка М.Ю. - К.: 2010. – ІССЗІ НТУУ «КПІ» – с.786, іл.
3. Уривський Л.О., Пешкін А.М. Методика оцінки граничної інформаційної ефективності завадостійких кодів// Information and Telecommunication Sciences, – К.: NTUU 'KPI'. – 2016. – № 2. – р.70-74.

ДОСЛІДЖЕННЯ НОВИХ КОМПОЗИТНИХ КОДІВ БАРКЕРА

Максимов В.В., Храповицький І.А.

*Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна**E-mail: maksimov46@ukr.net, hrpovitskiy.igor@gmail.com*

RESEARCH OF NEW COMPOSITE BARKER CODES

Modeling in the MatLab software package showed a greater noise immunity of new composite codes to the influence of various modulating sequences of an information signal in comparison with known composite codes.

Широкопasmові сигнали (ШСС) знаходять застосування в сучасних багатоканальних системах зв'язку з кодовим поділом каналів (CDMA, WCDMA), в системах бездротового зв'язку сімейства 802.11 з технологією розширення спектра методом прямої послідовності (Direct Sequence Spread Spectrum, DSSS), в сучасних радіолокаційних системах. З усіх ШПС найкращими кореляційними характеристиками володіють, відкриті в 1953 році, послідовності Баркера [1].

В [2] запропонований 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. В результаті перемноження короткої послідовності на довшу послідовність виходять послідовності понад 13 розрядів. Основний викид АКФ у них дорівнює числу розрядів результуючої послідовності N , а максимальний бічний викид в позитивну область має значення близькі до 1. В [3] шляхом формування складових кодових послідовностей аналогічно способу, запропонованого в [2], отримані 12 послідовностей з довжиною N , рівній 14 (14а, 14б), 21 (21а, 21б), 22 (22а, 22б), 33 (33а, 33б), 49, 77 (77а, 77б), 121, і перевищенням головного піку АКФ над позитивними бічними, рівним N . В [4] були запропоновані зворотні композитні коди Баркера, отримані перемноженням довгої послідовності на коротку, досліджена їх завадостійкість, і показана можливість їх використання в якості синхронізуючих слів в мережах WCDMA. В [5] описані ті ж складові кодові послідовності, що і в [3], але вже під назвою коди «Баркера-Волинської», і зазначено на можливість їх застосування, як для передачі команд, так і для синхронізації. В [6] показано, що АКФ композитних кодів Баркера, які формуються як скалярні добутки канонічних послідовностей Баркера [1, 7], можна записати як:

$$R_{\text{комп}}(k) = \frac{1}{m} \sum_{i=0}^m c_{\text{комп}}(i) c_{\text{комп}}(i+k) = \frac{1}{m} \sum_{i=0}^m c_{\text{комп.инв}}(i) c_{\text{комп.инв}}(i+k) = \\ = \frac{1}{m} \sum_{i=0}^m c_{\text{комп.зерк}}(i) c_{\text{комп.зерк}}(i+k) = \frac{1}{m} \sum_{i=0}^m c_{\text{комп.инв.зерк}}(i) c_{\text{комп.инв.зерк}}(i+k), \quad (1)$$

де $c_{\text{комп}}(i)$ – композитна послідовність Баркера, що визначається як

$c_{\text{комп}}(i) = c_1(i) c_2(i) \dots c_n(i)$, а $c_n(i)$ приймають значення ± 1 ;

$c_{\text{комп.инв}}(i) = (-1) c(i)$; $c_{\text{комп.зерк}}(i) = c_n(i) c_{n-1}(i) \dots c_1(i)$; $c_{\text{комп.инв.зерк}}(i) = (-1) c_{\text{комп.зерк}}(i)$.

В [6] також показано, що на підставі (1) композитні послідовності Баркера, отримані в [3], можна доповнити інверсними, дзеркальними і інверсними дзеркальними композитними послідовностями, які матимуть ті ж АКФ, що і основна композитна послідовність, тим самим збільшивши їх кількість з 12 до 48. Крім того в [6] отримані чотири пари нових композитних послідовностей Баркера, що мають одну і ту ж АКФ, що і 77б (номер послідовності узятий згідно [3]).

Нові композитні послідовності Баркера.

Використовуючи методику, викладену в [6], для кожної з композитних послідовностей 121, 77a, 49, 33a, 33b, 21a, 21b можуть бути знайдені по 4 пари сполучень основних послідовностей Баркера, що утворюють в цілому 28 нових композитних послідовностей, що мають однакову автокореляційну функцію з вихідними композитними послідовностями. У табл. 1 зведені всі 32 пари нових композитних послідовностей.

Таблиця 1. Нові композитні послідовності Баркера.

New №	Вариант	Новые композитные последовательности 121
New 1.	C11 x A11 D11 x B11	-1-1-1+1+1-1-1+1-1-1+1+1+1-1-1-1+1-1-1-1-1+1+1-1+1+1-1-1-1-1+1+1- 1+1+1-1-1+1+1-1-1-1+1-1-1-1+1+1-1+1+1-1-1-1+1+1-1+1+1-1-1-1- 1+1+1+1-1+1+1-1+1+1+1-1-1-1+1-1-1+1+1+1-1-1-1+1+1-1-1-1+1-1-
New 2.	C11 x B11 D11 x A11	+1+1+1-1-1-1+1-1-1-1-1+1+1-1+1+1-1+1+1+1-1-1-1+1-1+1-1+1+1-1-1+1- 1-1+1-1-1-1-1+1+1-1+1+1-1+1+1+1-1-1+1-1-1+1-1+1+1-1-1+1-1+1+1-1- 1-1+1-1-1+1-1-1-1+1+1+1-1+1+1-1+1-1-1+1+1-1+1+1-1+1+1-1+1+1-1+1
New 3.	A11 x C11 B11 x D11	-1+1-1-1+1-1-1+1+1+1-1+1-1-1+1+1-1+1-1-1+1-1-1+1+1+1-1+1+1- 1+1+1+1-1-1+1-1+1+1-1+1+1-1-1+1-1+1+1-1+1+1-1-1-1+1-1+1-1-1- 1+1+1+1+1-1+1+1-1+1+1-1-1+1-1+1+1-1+1+1-1-1-1+1-1-1+1+1+1-1+1+1- 1+1+1-1+1+1+1-1-1
New 4	A11 x D11 B11 x C11	+1-1+1+1-1+1+1-1-1-1+1-1+1+1-1+1+1-1-1-1+1+1-1+1+1-1-1-1+1-1-1-1- 1+1+1+1-1+1-1-1+1-1-1-1+1+1-1+1-1+1-1-1-1+1+1+1-1+1+1+1-1-1-1+1-1- 1+1-1-1-1+1+1-1+1-1+1-1-1-1+1+1+1-1+1+1-1+1+1-1-1-1+1+1+1-1+1+1+
№	Вариант	Новые композитные последовательности 77а
New 1.	C11 x A7 D11 x B7	-1-1-1+1+1+1 +1+1+1-1+1-1 -1-1+1+1+1 -1-1+1+1-1+1 +1+1+1-1+1-1 -1-1- 1+1+1-1+1-1-1+1+1-1+1 -1-1-1+1+1-1+1 +1+1+1-1+1-1 +1+1+1-1+1-1
New 2.	C11 x B7 D11 x A7	+1+1+1-1+1-1 -1-1+1+1-1+1 +1+1+1-1+1-1 +1+1+1-1+1-1 -1-1+1+1-1+1 +1+1+1- 1-1+1-1 +1+1+1-1+1-1 +1+1+1-1+1-1 -1-1+1+1-1+1 -1-1+1+1-1+1 -1-1+1+1-1+1
New 3.	A11 x C7 B11 x D7	-1+1-1-1+1+1 -1+1-1-1+1+1 -1+1-1-1+1+1-1+1+1-1-1 +1+1+1-1-1-1 +1-1+1+1- 1-1-1 -1+1-1-1+1+1+1-1+1-1-1 +1-1+1+1-1-1-1 -1+1-1-1+1+1+1-1+1+1-1-1
New 4	A11 x D7 B11 x C7	+1-1+1+1-1-1 +1-1+1+1-1-1 +1-1+1+1-1-1 -1+1-1-1+1+1-1 -1+1-1-1+1+1-1 -1+1-1- 1+1+1+1 +1-1+1+1-1-1-1 -1+1-1-1+1+1-1 -1+1-1-1+1+1+1-1+1+1-1-1-1 -1+1-1-1+1+1+1
№	Вариант	Новые композитные последовательности 77б
New 1.	C7 x A11 D7 x B11	-1-1-1+1+1+1-1+1+1-1+1+1+1-1-1+1-1+1-1-1-1+1+1-1+1+1-1+1-1-1+1+1- 1+1+1-1+1+1+1-1-1+1-1-1+1+1+1-1-1+1-1+1-1+1+1+1-1-1+1-1+1-1
New 2.	C7 x B11 D7 x A11	+1+1+1-1-1+1-1-1+1-1-1-1+1+1+1-1+1+1-1+1+1-1-1+1-1-1+1-1+1+1-1-1+1-1- 1-1+1-1-1-1+1+1+1-1+1-1-1-1+1+1-1+1+1-1-1-1+1+1+1-1+1+1-1+1
New 3.	A7 x C11 B7 x D11	-1+1-1-1+1-1-1-1+1+1+1-1+1-1-1+1+1-1+1-1+1-1-1+1+1+1-1+1+1- 1+1+1+1-1-1-1+1-1+1+1-1+1+1-1-1-1+1-1+1-1-1+1+1+1 +1-1+1+1-1+1+1-1-1-1
New 4	A7 x D11 B7 x C11	+1-1+1+1-1+1+1-1-1+1-1+1+1-1+1+1-1-1+1-1+1+1-1+1+1-1-1-1-1+1-1-1+1-1-1- 1+1+1+1-1+1-1-1+1-1-1+1+1+1-1+1+1-1+1+1-1-1-1-1+1-1-1+1+1
№	Вариант	Новые композитные последовательности 49
New 1.	C7 x A7 D7 x B7	-1-1-1+1+1-1+1+1+1-1+1-1-1-1+1-1+1-1-1+1+1-1+1+1+1-1+1-1+1+1+1-1- 1+1-1+1+1+1-1+1-1
New 2.	D7 x A7 C7 x B7	+1+1+1-1-1+1-1-1-1+1+1+1-1+1+1+1-1+1-1+1+1-1-1+1-1-1+1+1-1+1+1-1- 1+1-1-1+1+1-1+1
New 3.	A7 x C7 B7 x D7	-1+1-1-1+1+1+1-1+1-1-1+1+1-1+1-1+1+1+1-1+1-1-1+1-1-1+1+1-1-1-1+1-1- 1+1+1+1+1-1+1+1-1-1
New 4	B7 x C7 A7 x D7	+1-1+1+1-1-1-1+1-1+1+1-1-1+1-1+1+1-1-1+1-1-1+1+1-1+1-1+1+1+1-1- 1-1-1+1-1-1+1+1
№	Вариант	Новые композитные последовательности 33а
New 1.	C11 x A3; D11 x B3	-1-1+1 +1+1-1 -1-1+1 -1-1+1 +1+1-1 -1-1+1 -1-1+1 +1+1-1 +1+1-1 +1+1-1
New 2.	D11 x A3; C11 x B3	+1+1-1 -1-1+1 +1+1-1 +1+1-1 -1-1+1 +1+1-1 +1+1-1 +1+1-1 -1-1+1 -1-1+1 -1-1+1
New 3.	A11 x C3; B11 x D3	-1+1+1 -1+1+1 -1+1+1 +1-1-1 +1-1-1 +1-1-1 -1+1+1 +1-1-1 +1-1-1 -1+1+1 +1-1-1
New 4	B11 x C3; A11 x D3	+1-1-1 +1-1-1 +1-1-1 -1+1+1 -1+1+1 -1+1+1 +1-1-1 -1+1+1 -1+1+1 +1-1-1 -1+1+1
№	Вариант	Новые композитные последовательности 33б
New 1.	C3 x A11; D3 x B11	-1-1-1+1+1+1-1+1+1-1+1 +1+1+1-1-1+1-1-1+1-1 +1+1+1-1-1+1-1-1+1-1
New 2.	D3 x A11; C3 x B11	+1+1+1-1-1+1-1-1+1-1 -1-1-1+1+1+1-1+1+1-1+1 -1-1-1+1+1+1-1+1+1-1+1
New 3.	A3 x C11; B3 x D11	-1+1-1-1+1-1-1-1+1+1+1 -1+1-1-1+1-1-1-1+1+1+1 +1-1+1+1-1+1+1+1-1-1-1
New 4	B3 x C11; A3 x D11	+1-1+1+1-1+1+1+1-1-1 +1-1+1+1-1+1+1+1-1-1-1 -1+1-1-1+1-1-1-1+1+1+1

Таблиця 1 (продовження). Нові композитні послідовності Баркера.

№	Вариант	Новые композитные последовательности 21a
New 1.	C7 x A3; D7 x B3	-1-1+1 +1+1-1 -1-1+1 -1-1+1+1+1-1+1+1-1
New 2.	D7 x A3; C7 x B3	+1+1-1 -1-1+1 +1+1-1+1+1-1-1+1 -1-1+1 -1-1+1
New 3.	A7 x C3; B7 x D3	-1+1+1 -1+1+1 -1+1+1 +1-1-1 +1-1-1 -1+1+1 +1-1-1
New 4.	B7 x C3; A7 x D3	+1-1-1 +1-1-1 +1-1-1 -1+1+1 -1+1+1 +1-1-1 -1+1+1
№	Вариант	Новые композитные последовательности 21б
New 1.	C3 x A7; D3 x B7	-1-1-1+1+1-1+1 +1+1+1-1-1+1-1 +1+1+1-1-1+1-1
New 2.	D3 x A7; C3 x B7	+1+1+1-1-1+1-1 -1-1-1+1+1-1+1 -1-1-1+1+1-1+1
New 3.	A3 x C7; B3 x D7	-1+1-1-1+1+1+1-1+1-1-1+1+1+1 +1-1+1+1-1-1-1
New 4.	B3 x C7; A3 x D7	+1-1+1+1-1-1-1 +1-1+1+1-1-1-1 -1+1-1-1+1+1+1

Результати моделювання.

Для визначення можливості використання нових композитних кодів Баркера в якості синхроімпульсів необхідно, з одного боку, порівняти їх з відомими композитними кодами Баркера, а з іншого, в якості інформаційних сигналів вибрати такі, які створювали б для них найбільший рівень завад. Для моделювання в якості відомих композитних кодів були обрані вихідні композитні коди Баркера-Волинської [5], в якості інформаційних - вкладені коди Баркера, що мають такий же утворюючий код Баркера, що у відомих і нових композитних кодів.

Для моделювання була використана програма MATLAB R2015B. Схема моделі складалася з наступних основних функціональних вузлів: формувача широкосмугових сигналів; приймача синхросигналів; комутаторів режимів роботи.

Моделювання в середовищі MatLab показало, що нові композитні послідовності Баркера в розглянутих випадках використання в якості синхросигналів ефективніше вихідних кодів Баркера-Волинської, а саме:

- New1, New2, New3 і New4 (121 (11x11), 77a (11x7), 77b (7x11), 49 (7x7)) на (14,3 - 58,4)%;
- New1, New2, New3 (33a (11x3)) на (6,1 - 36,4)%;
- New2, New3 і New4 (33b (3x11)) на (36,4 - 69,7)%;
- New1, New2, New3 (21a (7x3)) на (9,5 - 38)%;
- New1, New2, New3 і New4 (21b (3x7)) на (9,5 - 47,7)%;

Нові композитні послідовності Баркера New2 і New3 (121 (11x11), 77a (11x7), 77b (7x11), 49 (7x7), 33a (11x3), 33b (3x11), 21a (7x3), 21b (3x7)) у всіх розглянутих випадках використання в якості синхросигналів ефективніше вихідних кодів Баркера-Волинської на (6,1 - 63,6)%.

Література

1. Barker, R. H. "Group Synchronizing of Binary Digital Sequences". Communication Theory. London: Butterworth. pp. 273–287.
2. Банкет В.Л., Токарь М.С. «Композитные коды Баркера» // Цифрові технології № 2, 2007р. С.8-17.
3. Волинская 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.
4. Максимов В.В., Чуприна Р.С. Обратные композитные коды Баркера // Наукові записки УНДІЗ, №1(21), 2012 г. – С.71-76.
5. Волинская А.В., Калинин П.М. Новые помехоустойчивые сигналы для интеллектуального канала телемеханики // Fundamental Research №11, 2012. – С.922-926.
6. Maksymov V., Khrapovitsky I. Research of composite Barker codes // The scientific heritage, № 48 (2020), P.1, p.p. 15-22.
7. Баскаков С.И. Радиотехнические цепи и сигналы: Учебник. М. Высш. школа, 1983. 536 с.

ВПЛИВ БАГАТОПРОМЕНЕВОСТІ НА КАНАЛ МОБІЛЬНОГО ЗВ'ЯЗКУ В ГІГАЕРЦОВОМУ ДІАПАЗОНІ ХВИЛЬ

Уривський Л.О., Солянікова В.Ю.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: leonid_uic@ukr.net

INFLUENCE OF MULTIPATH ON A MOBILE COMMUNICATION CHANNEL

This article describes the multipath nature of radio waves propagation in space during transmission from the base station to the receiver and power calculation of its influence.

У доповіді надано опис наслідків багатопроменевого характеру поширення радіохвиль у просторі при передачі від базової станції до приймача в гігагерцовому діапазоні хвиль і розрахунок потужності його впливу.

Поширення радіохвиль у вільному просторі, як правило, залежить від кількох факторів, незалежно від того, для чого призначений радіозв'язок. Серед основних факторів є втрати у вільному просторі з урахуванням шуму приймача, адитивних перешкод, а також мультиплікативних перешкод, причиною яких є багатопроменевий характер розповсюдження електромагнітних хвиль, що створюють перешкоди, тобто суперпозиція хвиль в приймачі.

Історія дослідження особливостей поширення радіохвиль розвивається в напрямку вектору потреб інформаційних систем в освоєнні все більш високих частот з метою забезпечення зростаючих швидкостей передавання інформації.

Зараз все більше уваги приділяється діапазону частот $f > 1$ ГГц, оскільки саме в цьому діапазоні працюють системи мобільного зв'язку 4G, 5G, а також сучасні безпроводові системи зв'язку [1-4].

В [1] надано опис особливостей багатопроменевого характеру поширення радіохвиль у просторі при передачі від базової станції до приймача і його вплив на передачу сигналу в діапазоні до 450 МГц. При цьому використовувалось моделювання розповсюдження хвиль за допомогою овалів Кассіні за методикою, запропонованою у [2].

Модель розповсюдження радіохвиль була побудована на припущенні, що область, яка суттєва для врахування впливу на приймальний пристрій відбитих від земної поверхні промінів, має форму окружності. Але точний розрахунок форми овалів Кассіні виявив, що ця область дещо сплюснута (рис. 1).

Формула для визначення параметра овалу Кассіні $a = \sqrt{R_1 R_2}$ в [2] має вигляд:

$$R_1 R_2 = \sqrt{(h_1^2 + h_0^2)(h_2^2 + h_0^2)} \sqrt{P_1 G_1 \eta_1 b_1 \eta_2 \omega_{\text{ВХ}} / U_{\text{ВХ}}}, \quad (1)$$

де $h_1 = 30$ м, $h_2 = 2$ м – висоти підвісу передавальної і приймальної антен,

$h_0 = 5$ м – мінімальна ефективна висота антени,

$P_1 = 40$ Вт – потужність передавача, $k = 0,6$ – коефіцієнт послаблення,

$G_1 = 18$ дБн = 63,1 – коефіцієнт посилення антени,

$\eta_1, \eta_2 = 0.9$ – коефіцієнти корисної дії системи передачі енергії від передавача до передавальної антени і навпаки,

$\omega_{\text{BX}} = 75 \text{ Ом}$ – вхідний опір приймача,

$U_{\text{BX}} = 0.7 \text{ мВ}$ – чутливість приймача (мобільного терміналу),

Параметр b_1 – це висота перешкоди, розташованого на відстані R_1 від мобільного терміналу (радіусу першої зони Френеля). Згідно [1], b_1 можна визначити по залежності:

$$b_1 = \sqrt{(\lambda R/3)k(1-k)} \quad (2)$$

де $R = 1 \text{ км}$ – відстань від передавальної до прийомної антени,

λ – довжина хвилі $\lambda = c/F$, де c – швидкість світла;

$F = 900 \text{ МГц}$ – частота, на якій передається сигнал.

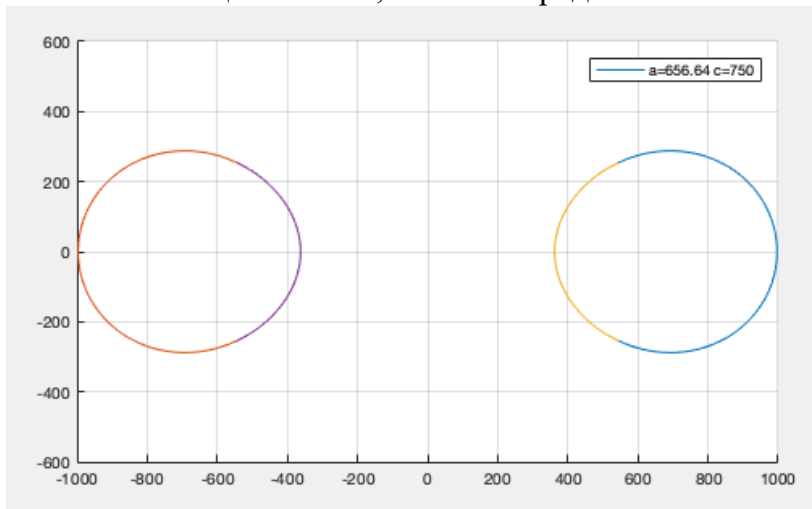


Рис.1. Побудова зони, суттєвої для відбиття додаткових променів для умови, що відстань між передавачем і приймачем $R = 1500 \text{ м}$, а частота, на якій передається сигнал, $f = 900 \dots 1500 \text{ МГц}$

Формула (1) є справедливою у випадку, коли виконується умова Релея (3) для відбиття променю від поверхні в проекції зони Френеля:

$$r_{[\text{км}]} \geq \frac{18h_{1[\text{м}]}h_{2[\text{м}]}}{\lambda} \quad (3)$$

Але для каналу зв'язку, що досліджується у даному випадку, ця умова не виконується, і більш того, зона Френеля не торкається рельєфу Землі (рис. 2).

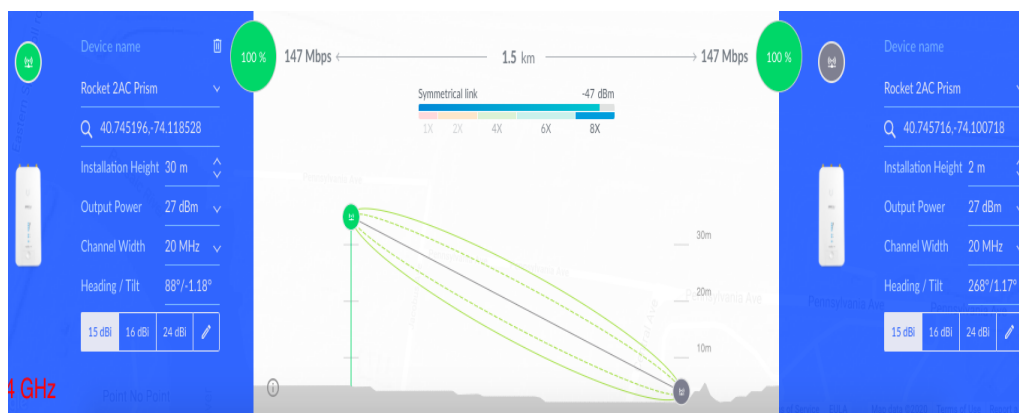


Рис.2. Побудова зони Френеля для каналу зв'язку що досліджується, для окремого випадку при відстані між передавачем і приймачем $R = 1500 \text{ м}$ та на частоті, на якій передається сигнал, $f = 2,4 \text{ ГГц}$

Отже, в такому випадку характеристики, пов'язані із висотою розташування антен вже не потрібні. Тому для розрахунку параметра овалу Кассіні $a = \sqrt{R_1 R_2}$ слід використовувати наступну формулу:

$$R_1 R_2 = \sqrt{\frac{k_0 P_T G_T G_R \lambda^4 \eta_T \eta_R}{(4\pi)^4 P_{R(\text{кр})}}}, \quad (4)$$

де G_T – коефіцієнт посилення приймальної антени, $G_R = 2$ – коефіцієнт посилення приймальної антени.

Ця формула дає змогу розрахувати параметр a і c (де $c = R/2$).

Результати розрахунків значень параметра a в різних діапазонах частот і при різній відстані від передавача до приймача (м), надано в таблиці 1.

Таблиця 1. Результати розрахунків.

Частота	900 МГц	2,4 ГГц	5 ГГц
Відстань R між передавачем і приймачем, м			
750	656,64	246,24	118,19
1000	656,64	246,24	118,19
1500	656,64	246,24	118,19

Для того, щоб порахувати сукупність потужностей прийнятих відбитих сигналів в точці прийому, необхідно проінтегрувати потужність в приймальному пристрої для всієї області, чутливої до прийому всіх відображених променів (рис.3).

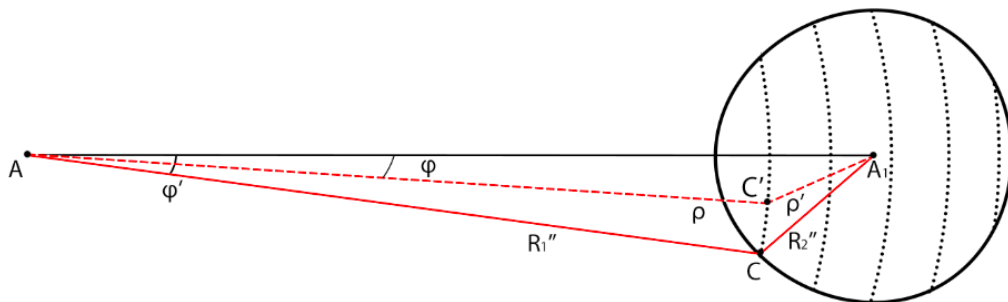


Рис.3. Побудова зони Френеля для каналу зв'язку, що досліджується, для окремого випадку при відстані між передавачем і приймачем $R = 1500$ м та на частоті, на якій передається сигнал, $f = 2,4$ ГГц.

Перш ніж потрапити в приймач, промінь виходить з передавача (точки А на рис. 3), відбивається від точки на деякій поверхні (припустимо це точка С), розсіюється, і тільки потім ослаблений потрапляє в точку прийому (точка A_1).

В такому випадку потужність сигналу в приймачі буде складатися з потужностей сигналів, відбитих від поверхонь, що потрапили в область,

суттєву для відбитих або розсіяних променів:

$$P_R = \frac{2P_T G_T G_R(\lambda)^4}{(4\pi)^4} \int_{R-R_2''}^{R+R_2'} \int_0^{\varphi(\rho)} \frac{1}{\rho^2(\rho^2 + R^2 - 2\rho R \cos \varphi)^2} d\varphi d\rho, \quad (5)$$

де ρ – це відстань, яку пройде додатковий (не прямий) промінь, перш ніж потрапити до приймача, а $\varphi(\rho)$ розраховується за формулою

$$\varphi(\rho) = \arccos \left\{ \frac{\rho^4 + R^2 \rho^2 - a^4}{2\rho^3 R} \right\} \quad (6)$$

Результати розрахунків потужності всіх відбитих променів в області чутливої до перешкод надано в таблиці 2.

Таблиця 2. Результати розрахунків потужності.

Частота Відстань R між А і А ₁ , м	900 МГц	2,4 ГГц	5 ГГц
750	-	1.5952e-05	5.0440e-06
1000	-	5.4056e-05	3.7764e-06
1500	5.9271e-14	1.0450e-06	1.6970e-06

При розрахунках для каналу зв'язку з частотою $f = 900$ МГц та відстанню між передавачем і приймачем 750 м і 1000 м, інтеграл розраховували не можливо, так як овал Касіні за таких параметрів приймає форму одного суцільного овалу, а не двох незалежних форм, як на рис. 1.

Інтеграл у формулі (5) дає можливість обчислити кількісні характеристики перешкоджаючих променів. Подальшою задачею є порівняння потужностей основного сигналу та завади в приймачі і розрахунок оптимальної кількості піднесучих OFDM, яка дасть можливість позбавитися від міжсимвольної інтерференції та послабити вплив багатопроменевості.

Література

1. Uryvsky L., Solianikova V, Method of Multipath Effect Elimination in Mobile Communications, / XIV Міжнародна науково-технічна конференція "Перспективи телекомунікацій 2020" /Збірник матеріалів. – К.: ІТС КПІ ім. Ігоря Сікорського, 2020, с.349...352.
2. Luchanin M., Chepkov I., Shmigel B. Analysis of spatial and energy limitations on the influence of multipath factors in the VHF radio channel model/ Conference: 2019 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo). – Режим доступу: <https://ieeexplore.ieee.org/document/9165402/>
3. Uryvsky L., Solianikova V, Analysis of Spatial-Time Characteristics of a Radio Line with Multipath within 5G Technology / Information and Telecommunication Science, . – № 1, 2020, с. 87...91. DOI: <https://doi.org/10.20535/2411-2976.12020.87-91>
4. Osypchuk S., Shmigel B., Moshynska A., Solyanikova V. Emergency ground communications system using 802.11xx technology / Conference: 2019 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo). – Режим доступу: <https://ieeexplore.ieee.org/document/9165476>.

**АПАРАТНО-ПРОГРАМНИЙ КОМПЛЕКС НА БАЗІ
МОДУЛЯТОРІВ DEKTEC ДЛЯ ФОРМУВАННЯ ТА ДОСЛІДЖЕННЯ
СИГНАЛІВ ЦИФРОВОГО ТЕЛЕВІЗІЙНОГО МОВЛЕННЯ**

Сливка А.Р., Авдєєнко Г.Л.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського

E-mail: aslivka61@gmail.com, djangoo2006@ukr.net

**HARDWARE AND SOFTWARE COMPLEX BASED ON
DEKTEC MODULATORS FOR THE GENERATION AND STUDY OF DIGITAL
TELEVISION BROADCASTING SIGNALS**

Implementation hardware and software complex based on Dektec modulators for the generation digital television broadcasting signals. Analysis the basic skills that can be acquired when working with it.

Сучасні системи кабельного, ефірного та супутникового телевізійного мовлення є складовою інфокомунікаційних мереж, які грають важливу роль в житті людини та розвитку суспільства. На даний момент інформація має статус одного з найважливіших стратегічних ресурсів, що має бути своєчасно доставлена до широкого кола користувачів. Таким чином, забезпечення кінцевого користувача якісними послугами, зокрема телевізійним контентом, є головною метою провайдера цих послуг. На даний момент часу в країнах Європи для вирішення цієї задачі використовуються цифрові сигнали різних стандартів таких, як DVB-T, DVB-T2, DVB-S, DVB-S2, DVB-C, DVB-C2 [1]. Станом на 2016 рік 166 країн світу прийняли стандарти DVB-T або DVB-T2 основними для цифрового ефірного наземного телемовлення. А такі стандарти супутникового телевізійного мовлення як DVB-S та DVB-S2 взагалі використовуються по всьому світу. Отже, актуальною стає задача теоретичної та, зокрема, практичної підготовки у вищих навчальних закладах фахівців, які матимуть ґрунтовні знання з сучасних систем цифрового телевізійного мовлення. Враховуючи, що вартість сучасних модулаторів цифрового телевізійного мовлення сягає тисяч та десятків тисяч доларів США, необхідно шукати шляхи створення для навчального процесу в університеті недорогих макетів, які дозволять розкрити всі особливості сучасних систем цифрового телевізійного мовлення.

Об'єктом дослідження у доповіді виступають системи цифрового ефірного та супутникового телевізійного мовлення, а предметом дослідження – процес формування сигналів цифрового ефірного та супутникового телевізійного мовлення стандартів DVB-T, DVB-S та DVB-S2 на базі модулаторів Dektec DTA-107 та Dektec DTA-115 [2,3]. Метою роботи є створення апаратно-програмного пристрою на базі модулаторів Dektec для більш детального і глибокого вивчення студентами ІТС методів формування та обробки сигналів цифрового ТВ мовлення.

Отже, в ході роботи було розроблено дві схеми макету, які можливо використовувати для дослідження сигналів цифрового мовлення. Ці схеми наведено на рис.1.

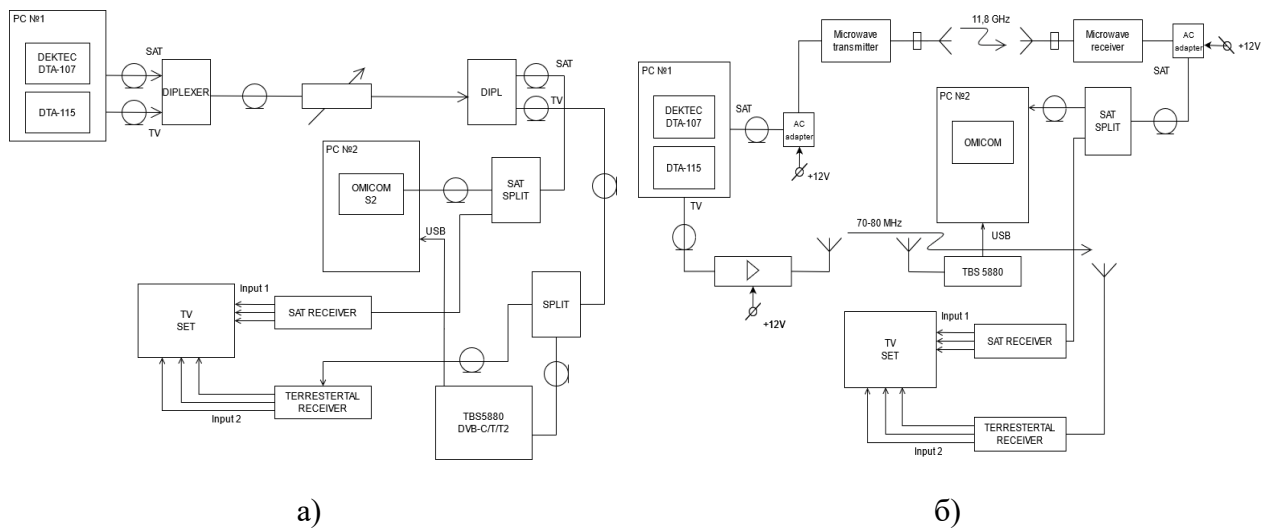


Рис. 1. Схеми для дослідження сигналів цифрового телевізійного мовлення на основі плат модуляторів Dektec DTA-107 (а) та Dektec DTA-115 (б).

Для управління PCI-платами модуляторів Dektec, які вставляються материнську плату ПК, використовується програмне забезпечення StreamXpress. Дана програма призначена для зчитування транспортного потоку або SDI-файлу з локального жорсткого диска ПК та підключення його до пристрою виведення DekTec для поточкового передавання в режимі реального часу. На рис.2 наведено головне меню ПЗ StreamXpress. У ньому можливо налаштувати основні параметри сигналу, обрати модулятор (Dektec DTA-107 або Dektec DTA-115), обрати файл транспортного потоку та клавіші управління відтворенням. Також є можливість більш детально переглянути інформацію про транспортний потік, та про сигнали відео та аудіо супроводу.

Для роботи з платою модулятора DTA-115 було обрано однопрограмний транспортний потік, центральна частота сигналу 586 МГц, полоса 8 МГц, тип модуляції QAM-64, стандарт цифрового мовлення DVB-T. Всі інші показники були залишені зі значеннями за замовчуванням. Зібравши схему яку зображено на рис. 1, а та додатково під'єднавши аналізатор спектру на один із виходів спліттера було отримано осцилограму сигналу цифрового мовлення стандарту DVB-T (рис. 3).

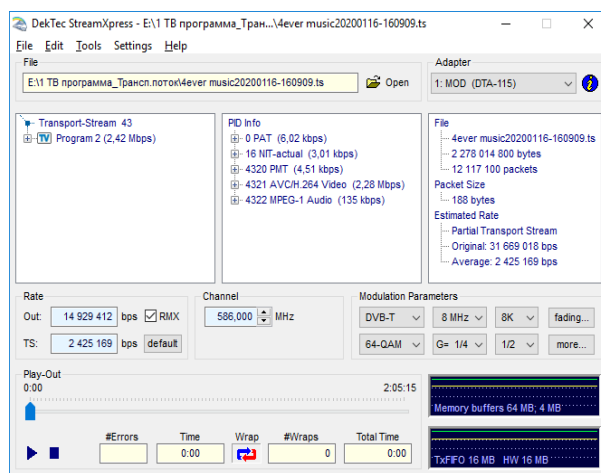


Рис.2. Головне меню програмного забезпечення StreamXpress.

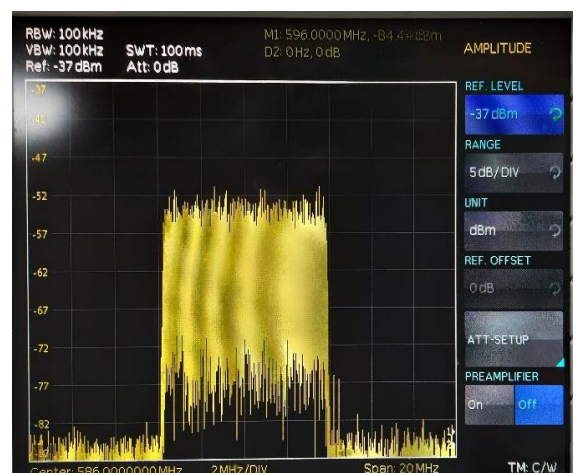


Рис.3. Радіопектр сигналу стандарту DVB-T на виході модулятора Dektec DTA-115.

Відповідно до схеми сигнал з виходу спліттера подається на вхід TBS5880, який є гібридним пристроєм для прийому сигналів стандарту DVB-T2/T та DVB-C і підключається до ПК за допомогою USB інтерфейсу. За допомогою ПЗ CrazyScan2 було проаналізовано спектр в діапазоні частот 560 – 596 МГц з кроком в 0,1 МГц. Та виконавши пошук сигналу на частоті 586 МГц з шириною 8 МГц та стандартом сигналу DVB-T, було отримано сигнальне сузір'я та основні параметри сигнал, який досліджується. (рис. 4).

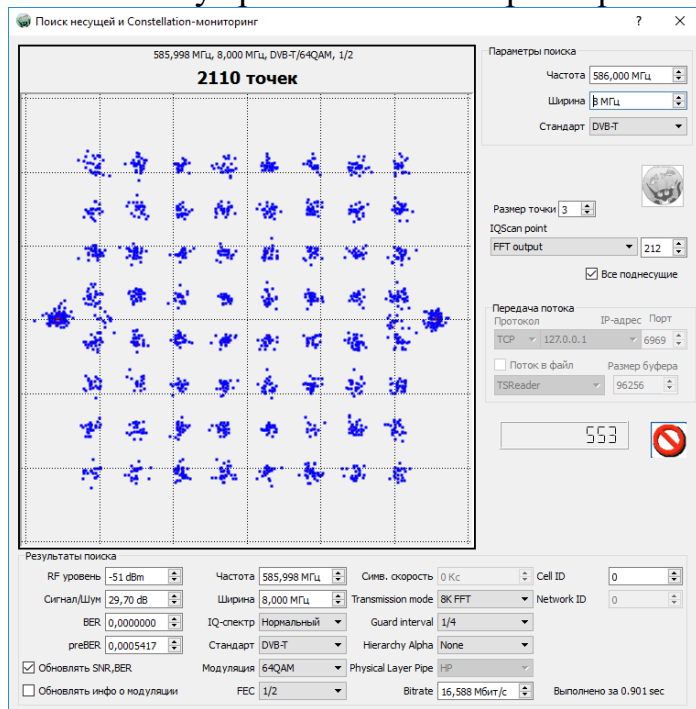


Рис. 4. Пошук сигналу за допомогою програмного забезпечення CrazyScan2.

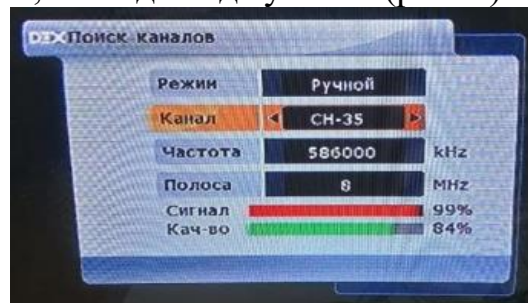


Рис.5. Параметри налаштування ресивера DEX стандарту DVB-T.



Рис.6. Програма на екрані ТВ, яку було передано.

Відповідно до останнього виходу спліттера було під'єднано ресивер стандарту DVB-T. Виконавши налаштування даного ресивера на частоту нашого сигналу (рис.5) та здійснивши пошук каналів ми отримали змогу переглянути програму (канал 4ever Music), яку ми передавали (рис.6).

Висновок. Отже за допомогою апаратно-програмного комплексу можливо детально дослідити параметри сигналів цифрового мовлення. Порівняти як саме ті чи інші параметри впливають на якість сигналу, його завадостійкість, дослідити сучасні багатопозиційні методи модуляцій. Отже на мою думку даний апаратно-програмний комплекс є можливістю для студентів закріпити та поглибити їх теоретичні знання з багатьох дисциплінах які вивчаються студентами ІТС.

Література

1. Карякин В.Л. Цифровое телевидение: учебное пособие для вузов, 2-е изд., переработанное и дополненное / В.Л. Карякин. - М: СОЛОН-ПРЕСС, 2013. - 448 с.
2. DTA-107 Satellite modulator for PCI [Електронний ресурс] – Режим доступу до ресурсу: <https://www.dektec.com/products/PCI/DTA-107/>.
3. DTA-115 Multi-standard cable/terrestrial modulator for PCI [Електронний ресурс] – Режим доступу до ресурсу: <https://www.dektec.com/products/PCI/DTA-115/>.

МОДЕЛЮВАННЯ 2-РЕЗОНАТОРНОГО ADD-DROP ФІЛЬТРА НА МІКРОКІЛЬЦЕВИХ РЕЗОНАТОРАХ

Пашенко А.І., Трубін О.О.

Інститут телекомунікаційних систем КІП ім. Ігоря Сікорського, Україна

E-mail: Andriypashenko@ukr.net

MODELING OF THE 2-RESONATOR ADD-DROP FILTER ON MICRORING RESONATOR

This publication is about a method for modeling of an Add / Drop filter based on an microring resonator transmission coefficients. The results of simulation of different types of filters are presented.

У роботі продемонстровано метод розрахунку параметрів ADD-DROP фільтрів різних типів із допомогою вирішення задачі розсіювання електромагнітних хвиль інтегральних оптичних ліній на системах зв'язаних між собою оптичних мікрорезонаторів.

Розвиток систем зв'язку відбувається у напрямку збільшення обсягів переданої інформації, що в свою чергу викликає потребу у зменшенні затримок та збільшення швидкостей передачі. При побудові сучасного телекомунікаційного обладнання все частіше виникає потреба переходу до більш високочастотних діапазонів, зокрема, міліметрового та терагерцового діапазонів довжин хвиль. Одні з ключових елементів інфраструктури мереж зв'язку - це фільтри. [1, 2]

У роботі продемонстровано метод розрахунку параметрів фільтрів різних типів (Чебишівський, Баттервортівський) з допомогою вирішення задачі розсіювання електромагнітних хвиль інтегральних оптичних ліній на системах зв'язаних між собою оптичних мікрорезонаторів.



Рис.1. Схема 2-резонаторного фільтру.

На рис.1 зображено фільтр який складається з резонаторів (R1, R2) та двох хвилеводних трактів (1-2 та 3-4), де 1 - порт введення сигналу, 2 - порт виведення підсиленого сигналу, 3 - порт видалення, 4 - порт додавання.

Коефіцієнт зв'язку для фільтру, зображеного на рис. 1, можна отримати з [3], і для випадку з двома резонаторами він має вигляд:

$$K = \|k_{s2}(1 - \delta_{s2}) + i(\tilde{k}_1^e \delta_{s1} + \tilde{k}_1^0 \delta_{s2} + \tilde{k}_2^e \delta_{s3} + \tilde{k}_2^0 \delta_{s4} + \tilde{k}_{os})\|, \quad (1)$$

де $\tilde{k}_N^e$ - коефіцієнт зв'язку мікрорезонатора з лінією зв'язку для парних

коливань; $\tilde{k}_N^o$ - коефіцієнт зв'язку мікрорезонатора з лінією зв'язку для непарних коливань; k_{s2} - коефіцієнт взаємного зв'язку мікрорезонаторів; $\tilde{k}_{os}$ - коефіцієнт зв'язку мікрорезонаторів з відкритим простором; δ_s - символ Кронекера.

Параметри матриці розсіювання на вході (виході) фільтра можна розрахувати використовуючи відомі [4] вирази:

$$S_{1v} = 20\log(|T_{1v}|) = 20\log(|(\delta_{2v} - \frac{Q^D}{\det B} \sum_{s=1}^{2N} \frac{\det B_v^s}{Q_s(\omega)})|), \quad (2)$$

де

$$B_v^s = \begin{bmatrix} b_1^{e1} & \dots & \sum_{n=1}^n b_n^{es} \tilde{k}_{n1}^{++} & \dots & b_1^{e2N} \\ b_1^{o1} & \dots & \sum_{n=1}^n b_u^{es} \tilde{k}_{n1}^{++} & \dots & b_1^{o2N} \\ \vdots & & \vdots & & \vdots \\ \vdots & b_N^{o1} & \dots & 0 & \dots & b_N^{o2N} \end{bmatrix}, \quad (3)$$

$$B(\omega) = \begin{bmatrix} b_1^{e1} & \dots & b_1^{e2N} \\ b_1^{o1} & \dots & b_1^{o2N} \\ \vdots & & \vdots \\ b_N^{o1} & \dots & b_N^{o2N} \end{bmatrix}, \quad (4)$$

$$Q_s(\omega) = \frac{f}{f_0} + 2iQ^D \left(\frac{f}{f_0} - 1 - \frac{\lambda_s}{2} \right), \quad (5)$$

Q^D – добротність мікрорезонатора, N – кількість резонаторів, λ_s – власні значення матриці K , f_0 – частота власних коливань ізолюваних мікрорезонаторів.

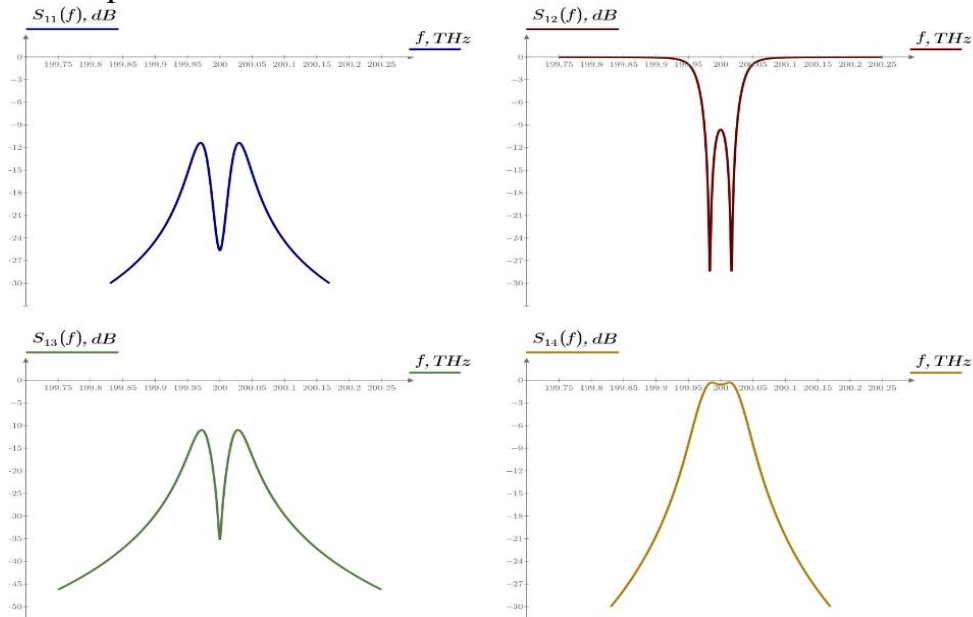


Рис. 2. Результат розрахунків матриць розсіювання 2 резонаторного Add-Drop фільтра.

Результати розрахунку залежності матриці розсіювання від частоти для 2-резонаторного Add-Drop фільтра наведені на рис. 2. Значення, використані

при розрахунках: $f_0 = 200$ ТГц; $Q^D = 10^6$; $\tilde{k}_{OS} = 10^{-7}$; $\tilde{k}^e = 1.5 \cdot 10^{-4}$; $\tilde{k}^0 = 2 \cdot 10^{-4}$; $k_{12}^e = k_{21}^e = 2 \cdot 10^{-4}$; $k_{12}^0 = k_{21}^0 = -3 \cdot 10^{-4}$.

В результаті розрахунків отримано фільтр, з квазі-Чебишівською характеристикою АЧХ на виході 4. Отримані розрахунки відповідають отриманим у роботі [5]. Варіюючи коефіцієнти зв'язку фільтрів з лініями передачі та коефіцієнти зв'язку фільтрів R1 з R2 можна бачити, що використовуючи коефіцієнти:

- $\tilde{k}^e = 2 \cdot 10^{-4}$, $\tilde{k}^0 = 2.5 \cdot 10^{-4}$, $k_{12}^e = k_{21}^e = 2 \cdot 10^{-4}$,
 $k_{12}^0 = k_{21}^0 = -3 \cdot 10^{-4}$ можна отримати Баттервортівську характеристику (гладка характеристика у смузі пропускання, найменша крутизна спаду – рис. 3,а);
- $\tilde{k}^e = 2 \cdot 10^{-4}$, $\tilde{k}^0 = 0.5 \cdot 10^{-4}$, $k_{12}^e = k_{21}^e = 1 \cdot 10^{-4}$,
 $k_{12}^0 = k_{21}^0 = -3 \cdot 10^{-4}$ можна отримати Чебишівську характеристику 1-го роду (з пульсацією у смузі пропускання, середнє значення крутизни спаду – рис. 3,б).

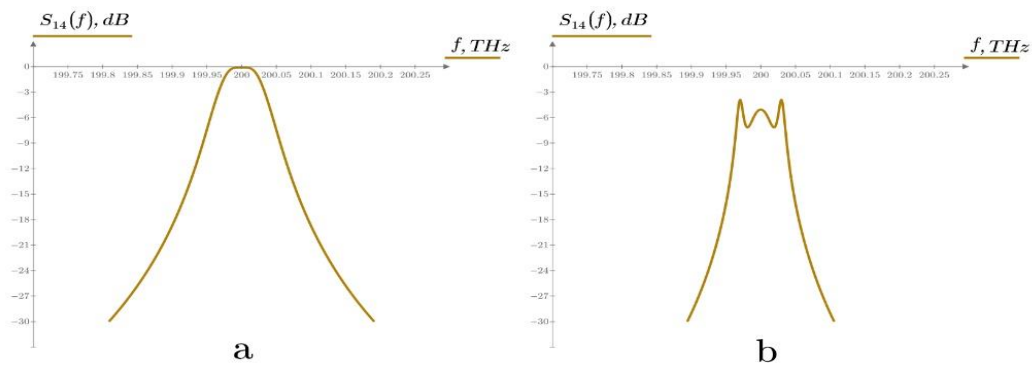


Рис. 3. Варіювання коефіцієнтів зв'язку Add-Drop фільтра.

У результаті моделювання продемонстровано можливість розрахунку фільтрів різного типу за допомогою запропонованої моделі. Отримані дані підтверджують можливість застосування моделі для майбутнього проектування оптичних фільтрів.

Література

1. Підгурська Т.В. Двосмугові фільтри на діелектричних резонаторах з вищими типами коливаний: автореф. дис. канд. техн. наук.: 05.12.13 – радіотехнічні пристрої та засоби телекомунікацій / Тетяна Василівна Підгурська. - Київ, 2016. - 24 с. <https://ela.kpi.ua/handle/123456789/15380>
2. Городецкий М. Л. Оптические микрорезонаторы с гигантской добротностью. — М.: ФИЗМАТЛИТ, 2011. - 416 с.
3. Trubin A.A. Lattices of Dielectric Resonators, Springer International Publishing Switzerland. Series in Advanced Microelectronics 53, 2016. <https://link.springer.com/book/10.1007%2F978-3-319-25148-6>. <https://doi.org/10.1007/978-3-319-25148-6>.
4. Trubin A. A. Electrodynamics modeling of add-drop filters on optical microresonators, 2019, pp. 30–36, DOI: <https://doi.org/10.20535/2411-2976.12019.30-36>.
5. Trubin A. A. Calculation parameters of add-drop filters on optical microresonators, <http://conferenc.its.kpi.ua/2019/paper/view/15706/8569>.

MICROWAVE FILTERS WITH VARIABLE PARAMETERS BASED ON CELLS OF METAMATERIALS

Zhivkov A., Akopian P., Galickiy I., Krylach O., Kopaniev M., Kamarali R.

National Technical University of Ukraine

“Igor Sikorsky Kyiv Polytechnic Institute”

Institute of Telecommunication systems

E-mail: ilyagal26@ukr.net

МІКРОХВИЛЬОВІ ФІЛЬТРИ ІЗ ЗМІННИМИ ПАРАМЕТРАМИ НА БАЗІ КОМІРОК МЕТАМАТЕРІАЛІВ

У доповіді розглянуті способи управління смугами пропускання і режекції мікрохвильових фільтрів на базі комірок метаматеріалів. Розглянуто особливості перебудови парних і непарних мод коливань в залежності від місця підключення варакторів. Моделювання проводилося за допомогою програмних продуктів Microwave Office.

The report considers ways to control the bandwidth and selectivity of microwave filters based on cells of metamaterials. Peculiarities of even and odd modes of oscillations depending on the place of connection of varactors are considered. The simulation was performed using Microwave Office software products.

Microwave filters with controlled characteristics are widely used in modern telecommunications technology, and numerous publications in modern literature are devoted to their study [1-7]. In [8], a design of a bandpass microstrip filter with a controllable passband was proposed, which, as it is now found out [9, 10], can be classified as “cells of a metamaterial with controllable characteristics” (control of odd mode parameters). Investigation of metamaterials with controllable characteristics and filters based on them are devoted to works [11-13].

The purpose of our report is to select the optimal method for controlling the parameters of the cells of metamaterials both in band-stop and bandpass filters. Let us first of all consider the control of vibration modes of a metamaterial cell using varactors. In the microwave range, take into account that a varactor is not just a variable capacitance, but a 2-pole with its own “useful” and “parasitic” parameters [14]. In fig. 1 a) shows a model of a notch filter (AWR software environment) with a varactor connected in the middle of the microstrip resonator, and fig. 1 b) parameter S_{21} of the filter at different values of the varactor capacitance (capacitance C is indicated in the figure in pF). The most important feature of this method of turning on the varactor is that one (first, which is also odd) harmonic “remains in place”, while the second harmonic is rearranged significantly and at $C = 3.1$ pf it approaches the first harmonic so much that the Fano resonance mode is realized.

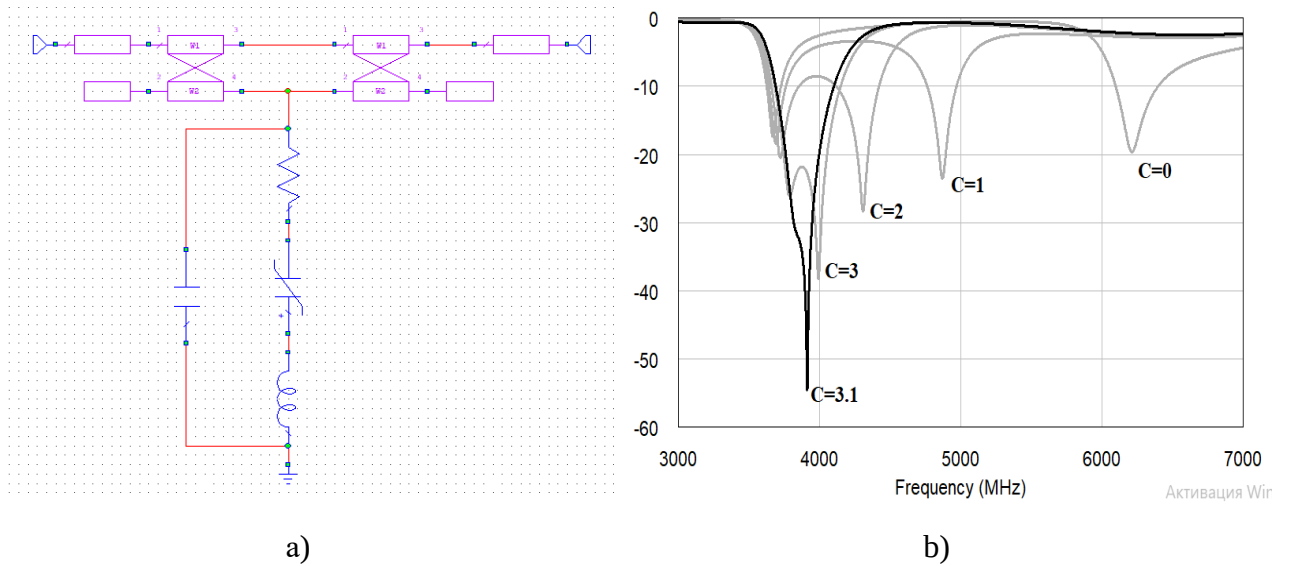


Fig 1. Tuning of the "even" harmonic of the microstrip resonator.

To tune the odd harmonics (first and third), we include a varactor in the gap of the microstrip resonator in Fig. 2 a). In fig. 2 b) are presented filter characteristics at different values of the varactor capacitance (capacities are indicated in the figure in pF).

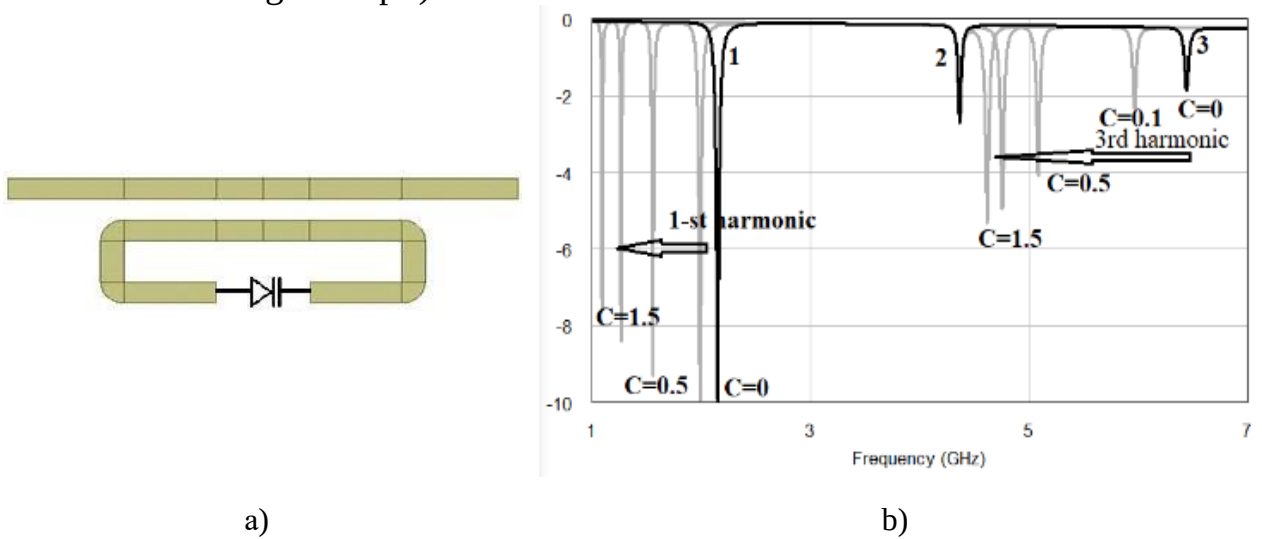


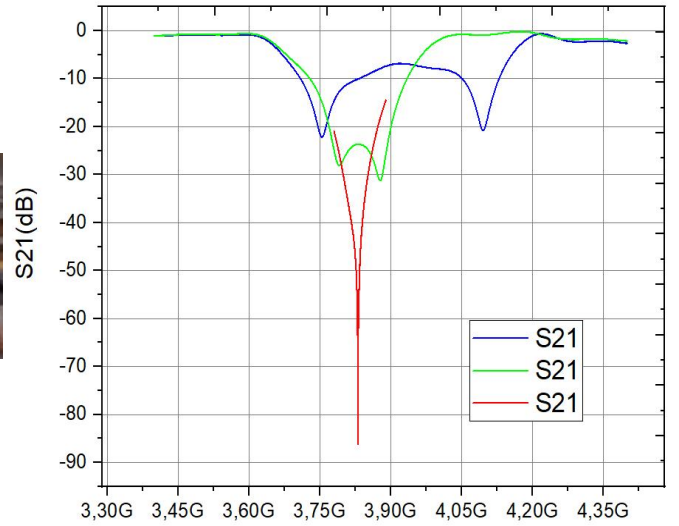
Fig. 2. Tuning of "odd" harmonics of a microstrip resonator.

We observe, as expected, the rearrangement of the "odd" 1st and 3rd harmonics, the second harmonic ("even") does not change with this method of switching on the varactor.

Other methods of tuning the frequency of microstrip resonators are also known. In the process of fine tuning the band-stop filters to obtain anomalously high levels of attenuation (Fano resonance) and group delay (GD), we used a dielectric plate with a permittivity not exceeding the permittivity of the substrate (Fig.3a). The more the plate "covers" the resonator, the lower its resonant frequency. Approaching the resonant frequency of the short resonator ("odd" mod) to the resonant frequency of the long resonator (even mod), we also achieve the Fano resonance, as shown in Fig. 3.b).



a)



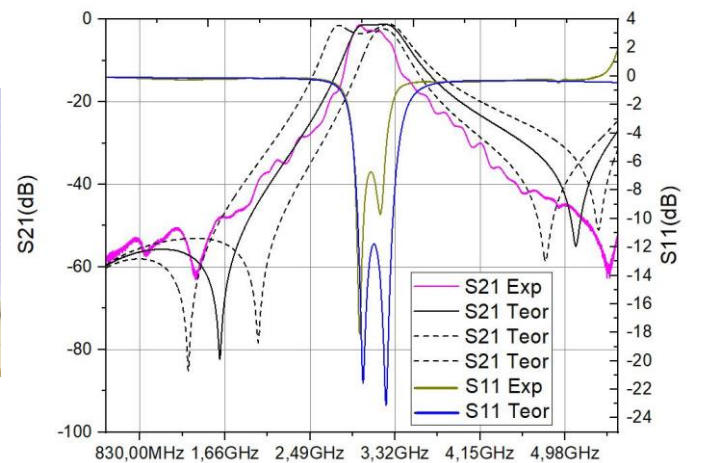
b)

Fig. 3. Tuning the "cell of the metamaterial" using a dielectric plate.

Let us note one more way of influencing the characteristics of filters based on metamaterial cells of some elements of its design. If, in the bandpass filter investigated in [15], we change the real thickness of the wire, which provides a short circuit of the "long" resonator, that is, in fact, its parasitic inductance, then it is possible to quite effectively regulate its bandwidth and the position of the damping poles, as demonstrated in fig. 4. The dotted line shows the theoretical curves of the transmission coefficient S_{21} (the diameter of the wire providing the short circuit varies from about 5 to 2 mm), the "theoretical" solid lines for S_{21} and S_{11} (the wire diameter is 1 mm) are in good agreement with the experimental results.



a)



b)

Fig. 4. Layout of a band-pass microstrip filter (Fig. A) [15] and its characteristics for different parameters of the parasitic inductance of the short-circuit wire.

References

1. A. R. Brown and G. M. Rebeiz, A Varactor-Tuned RF Filter Ieee Transactions On Microwave Theory And Techniques, vol. 48, no. 7, July 2000 DOI: 10.1109/22.848501.
2. H. Lee and S. Yun, Microwave Planar Varactor Tuned Bandpass Filters: Historical Overview Ieee Transactions on Electronics 2006/12/01 vol.E89-C, no.12 pp.1806-1813 DOI:10.1093/ietele/e89-c.12.1806.
3. C. Musoll-Anguiano, I. Llamas-Garro, Z. Brito-Brito, L. Pradell and A. Corona-Chavez, Fully Adaptable Band-Stop Filter Using Varactor Diodes Microwave And Optical Technology Letters, vol. 52, no. 3, March 2010 DOI: 10.1002/mop.24969.
4. W. Tang and J. Hong, Varactor-Tuned Dual-Mode Bandpass Filters September 2010 IEEE Transactions on Microwave Theory and Techniques 58(8):2213 – 2219 doi:10.1109/tmtt.2010.2052958.
5. A. V. Zakharov and M. Ye. Ilchenko, Varicap-Tuned Narrowband Filters with Extended Rejection Band Based on U-shaped Microstrip Resonators Radioelectronics and Communications Systems, 2017, vol. 60, no. 9, pp. 383–392. © Allerton Press, Inc., 2017 DOI: <https://doi.org/10.3103/S0735272717090011>.
6. Alexander Zakharov et al.: Varactor-Tuned Microstrip Bandpass Filter with Loop Hairpin and Comblaine Resonators IEEE Transactions on Circuits and Systems II: Express Briefs (Volume: 66, Issue: 6, June 2019) DOI: 10.1109/TCSII.2018.2873227.
7. B. Pal and S. Dwari, Harmonic Suppressed Tunable Bandpass Filter Using Varactor-Tuned Stub-Loaded Resonator, IETE Journal of Research, 2019, DOI: 10.1080/03772063.2019.1700176 USSR Inventor's Certificate 1518837.
8. M. Ilchenko, A. Zhivkov, A. Zazerin, Metamaterial Cells Equivalent Circuit, Degenerated Oscillation and Electromagnetically Induced Transparency 2018 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo) September 10-14, 2018, Odessa, Ukraine DOI: 10.1109/UkrMiCo43733.2018.9047596.
9. 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.
10. A. Genc and R. Baktur, A Tunable Bandpass Filter Based On Varactor Loaded Split-Ring Resonators Microwave And Optical Technology Letters, vol. 51, no. 10, October 2009 <https://doi.org/10.1002/mop.24641>.
11. T. Nesimoglu and C. Sabah, A Tunable Metamaterial Resonator Using Varactor Diodes to Facilitate the Design of Reconfigurable Microwave Circuits Ieee Transactions On Circuits And Systems—II: Express Briefs, vol. 63, no. 1, January 2016 DOI: 10.1109/tcsii.2015.2503058.
12. M. Maasch, Tunable Microwave Metamaterial Structures Springer, 2016, DOI 10.1007/978-3-319-28179-7.
13. G. H. Stauffer, Finding the Lumped Element Varactor Diode Model. November 2003 High Frequency Electronics.
14. M. Ilchenko et al: Attenuation Poles In Band-Pass Filters With Even End Odd Modes. Proceedings of the International Scientific and Technical Conference "Prospects for Telecommunications", [S.l.], May. 2020. ISSN 2664-3057 online. DOI: <http://conferenc.its.kpi.ua/proc/article/view/201713>.

DESIGN AND OPTIMIZATION OF TWO-RESONATOR INSET-FED PRINTED 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 ДВОРЕЗОНАТОРНОЇ ДРУКОВАНОЇ ПАТЧ-АНТЕНИ ІЗ ЗАГЛИБЛЕНИМ ЖИВЛЕННЯМ ДЛЯ ЧАСТОТНОГО ДІАПАЗОНУ 2,4 ГГц

Здійснено проектування та оптимізацію дворезонаторної друкованої патч-антени діапазону 2.4 ГГц. Один резонатор є активним та збуджується мікросмужковою лінією, заглибленою в нього. Другий резонатор є пасивним та збуджується за допомогою електромагнітного зв'язку з активним резонатором. Проведено моделювання роботи антени методом скінченних елементів в діапазоні робочих частот 2.4...2.483 ГГц. В результаті оптимізації антени збільшено смугу її пропускання та покращено узгодження у смугі робочих частот. В межах робочої смуги частот КСХ розрахованої антени знаходиться в діапазоні 1...1.7.

Development of mobile communication systems increases the demand for small-size and high-performance microwave antennas. 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 their design and fabrication [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 the analytical model and the FEM simulation was done in [4] for a 2.4 GHz single-resonator patch antenna.

In this paper, a microstrip two-resonator rectangular inset-fed patch antenna for the 2.4 GHz band is designed and simulated using the finite-element method. Single-resonator patch antennas were considered in [5], [6]. However, they have a resonance-like frequency response. Adding of additional resonator allows to increase antenna bandwidth.

The antenna to be designed should operate in the frequency range 2400...2483 MHz, which is one of ISM 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, an additional parasitic patch was added to the antenna design. As a substrate for the antenna, the RT/Duroid 5880 laminate was used with the following parameters: dielectric constant $\epsilon_r = 2.2$; thickness $h = 1.575$ mm; thickness of the top and bottom copper layers $t = 0.018$ mm; dissipation is defined by $\tan \delta = 0.0009$.

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 microstrip 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.

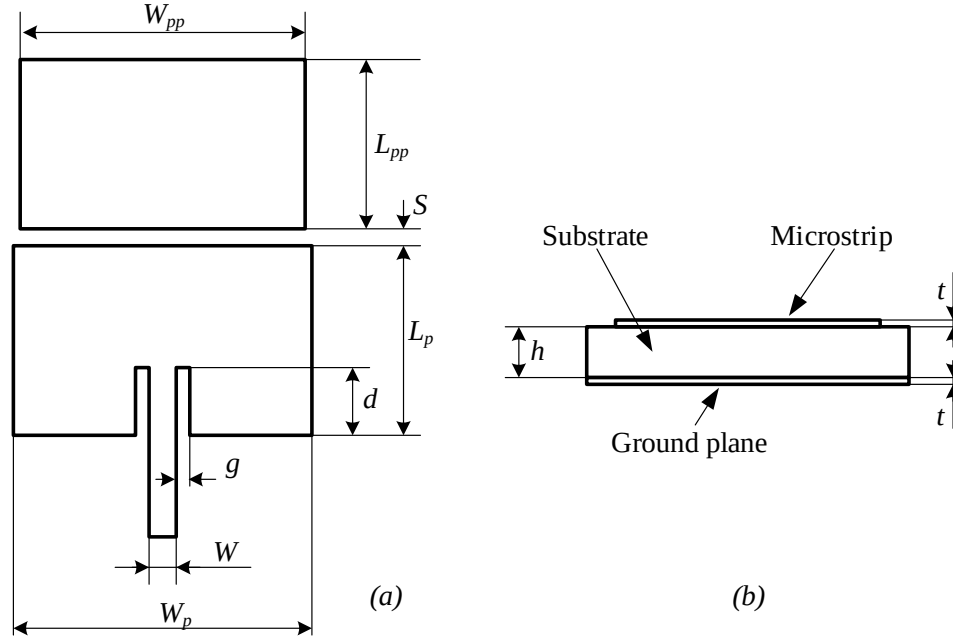


Fig.1. Dimensions of a microstrip patch antenna.
(a) Dimensions of the microstrip patches.
(b) Dimensions of the substrate and copper layers.

The design procedure described in [1] and [4] was used to obtain the initial values of the dimensions of the patch, which are as follows: width of the patch $W_p = 48.56$ mm; length of the patch $L_p = 40.64$ mm; inset distance $d = 14.25$ mm; notch width $g = 0.28$ mm. The width of the feeding line strip was chosen to be $W = 4.9$ mm in order to perform the characteristic impedance of the line to be $Z_0 = 50 \Omega$.

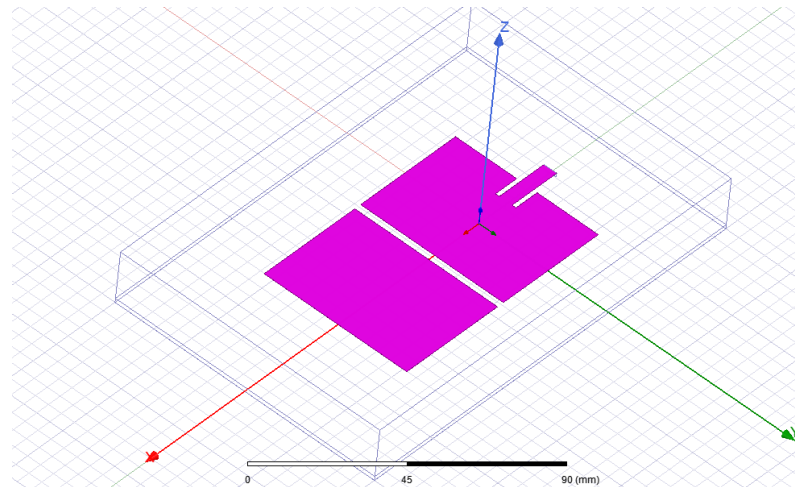


Fig.2. Model of the antenna.

After the optimization procedure the following dimensions were chosen for the antenna: $W_p = W_{pp} = 55$ mm; $L_p = 40.3$ mm; $d = 9$ mm; $S = 2.5$ mm; $L_{pp} = 38.5$ mm; $g = 1.5$ 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 $RL = |S_{11}| \approx -12$ 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 $RL = |S_{11}| \approx -22$ dB at the centre frequency $f_0 = 2.442$ GHz. The gain of the antenna is $G = 8.6$ dB. The polarization of the antenna is linear.

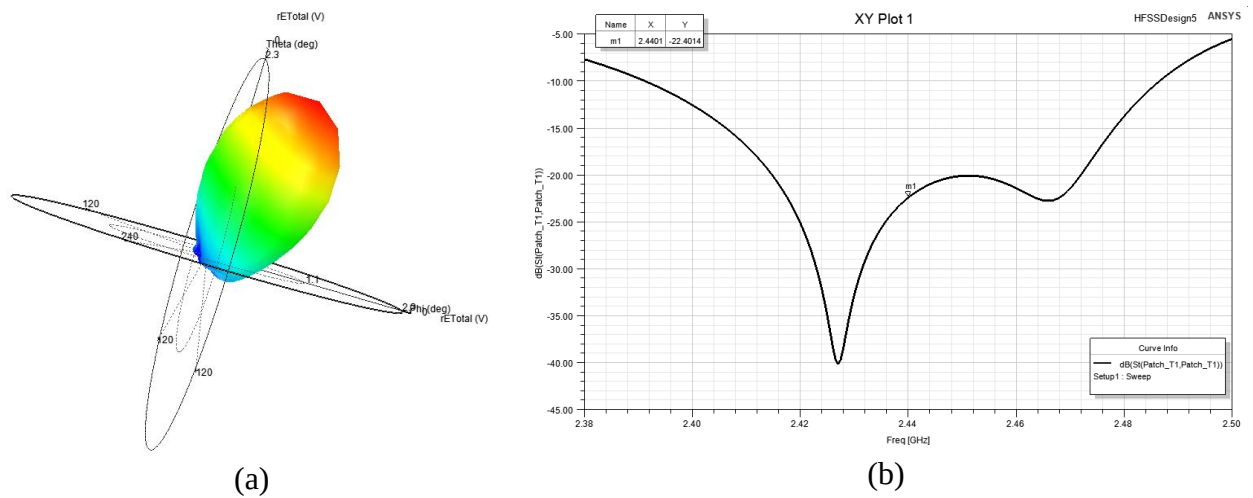


Fig.3. Characteristics of the antenna. (a) Directivity. (b) Return loss.

The antenna designed in the present research is small-sized and easily fabricated. Adding an additional parasitic rectangular patch resonator positioned next to the active resonator lead to the relatively high bandwidth of the antenna comparing with the one studied in [4]. The bandwidth at the level of $RL = -12$ dB is $\Delta f = 83$ MHz, i.e. VSWR within the required bandwidth is in the range $1 \dots 1.7$.

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. 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>.
5. Trubarov I.V. Design and Optimization of Coaxial-Fed Rectangular Patch Antenna for 2.4 GHz Frequency Band \ XIV International Scientific Conference "Modern Challenges in Telecommunications" MCT-2020. Conference proceedings. Kyiv. Igor Sikorsky Kyiv Polytechnic Institute, 2020 – pp. 68 – 70. – ISSN(print)2663-502X.
6. Trubarov I.V. Design and Optimization of Coaxial-Fed Circular Patch Antenna for 2.4 GHz Frequency Band \ XIV International Scientific Conference "Modern Challenges in Telecommunications" MCT-2020. Conference proceedings. Kyiv. Igor Sikorsky Kyiv Polytechnic Institute, 2020 – pp. 74 – 76. – ISSN(print)2663-502X.

DESIGN AND OPTIMIZATION OF COAXIAL-FED RECTANGULAR TWO-RESONATOR 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 ДВОРЕЗОНАТОРНОЇ ПРЯМОКУТНОЇ ПАТЧ-АНТЕНИ З КОАКСІАЛЬНИМ ЖИВЛЕННЯМ ДЛЯ ЧАСТОТНОГО ДІАПАЗОНУ 2,4 ГГц

Здійснено проектування та оптимізацію двореzonаторної прямокутної 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 антени збільшено смугу її пропускання за рахунок електромагнітного зв'язку між активним та пасивним резонаторами антени. В межах робочої смуги частот КСХ розрахованої антени перебуває в діапазоні 1...1.4.

Development of mobile communication systems and IoT-devices increases the demand for small-size and high-performance microwave antennas. At present, theory of antenna design is well-studied part of microwave engineering covering a large number of small-size antenna types and design techniques that can be used for their design [1] – [3]. Antenna design is typically an iterative procedure involving numerous simulations to optimize its parameters. 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 the analytical model and the FEM simulation was done in [4] for a 2.4 GHz patch antenna.

In this paper, a microstrip rectangular coaxial-fed patch antenna for 2.4 GHz band is designed and simulated using the finite-element method.

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 center 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 $h_p = 2$ mm; thickness of the top and bottom aluminium layers $t = 0.5$ mm.

The topology of the antenna with the dimensions of the patches 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.

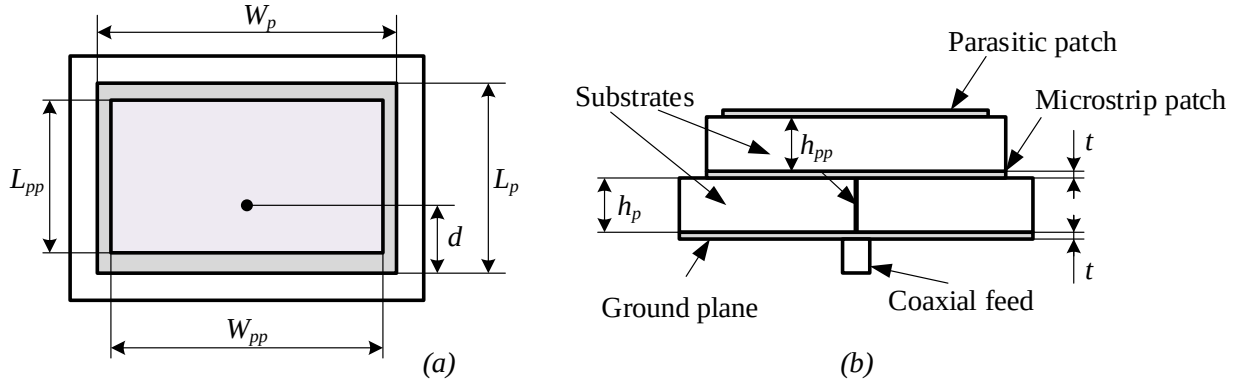


Fig.1. Dimensions of a microstrip patch antenna. (a) Dimensions of the microstrip patch. (b) Dimensions of the substrate and aluminium layers.

The design procedure described in [1] – [3] was used to obtain the initial values of the dimensions of the patch, which are as follows: width of the patch $W_p = 62$ mm; length of the patch $L_p = 56$ mm; inset distance $d = 18$ 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. A parasitic resonator was added to antenna, and the whole structure was simulated using finite-element numerical method. Single-resonator patch antennas were considered in [5], [6]. However, they have a resonance-like frequency response. Adding of additional resonator allows to increase antenna bandwidth.

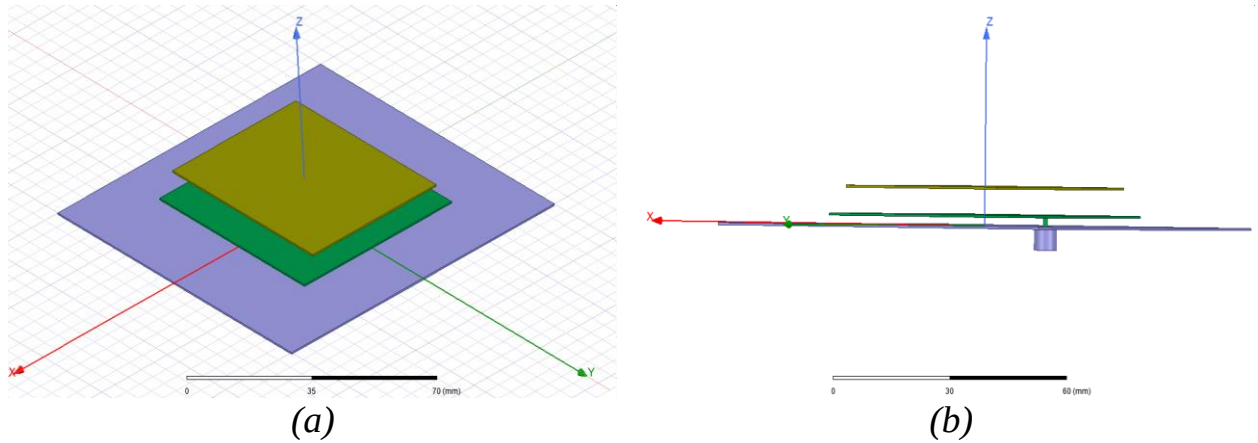


Fig.2. Model of the antenna. (a) Upper view. (b) Side view.

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; $W_{pp} = 60$ mm; $L_p = 56$ mm; $L_{pp} = 47$ mm; $d = 9$ mm. In Fig.3, the simulated results for the directivity diagram and the frequency response

of the antenna are shown. As it could be seen, the return loss is $RL = |S_{11}| \approx -16$ dB at the left band edge ($f_L = 2.4$ GHz), and $RL = |S_{11}| \approx -22.3$ dB at the right band edge $f_R = 2.483$ GHz, and $RL = |S_{11}| \approx -19$ dB at the center frequency $f_0 = 2.442$ GHz. The gain of the antenna is $G = 9.3$ dB. The polarization of the antenna is linear with $\mathbf{E}$ vector oriented in XZ-plane, as shown in Fig. 2.

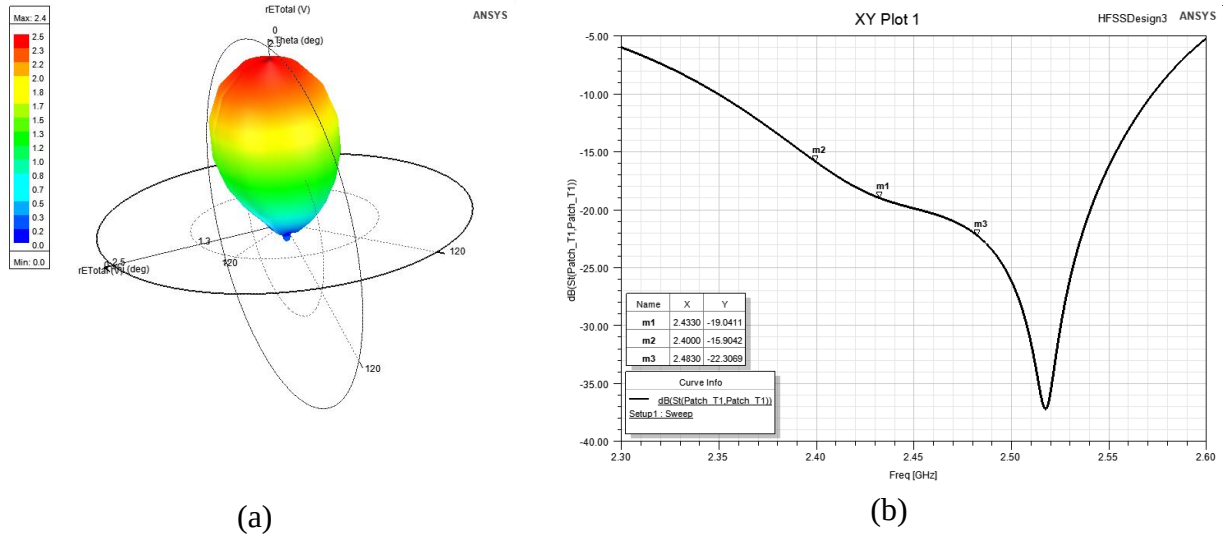


Fig.3. Characteristics of the antenna. (a) Directivity. (b) Return loss.

The antenna designed in the present research is small-sized and easily fabricated. Adding a parasitic resonator as small value of dielectric constant $\epsilon = 1$ lead to the relatively high bandwidth of the antenna comparing with the one studied in [5]. VSWR value within the operating bandwidth 2.4...2.483 GHz is in the range 1...1.4.

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. 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>.
5. Trubarov I.V. Design and Optimization of Coaxial-Fed Rectangular Patch Antenna for 2.4 GHz Frequency Band \ XIV International Scientific Conference "Modern Challenges in Telecommunications" MCT-2020. Conference proceedings. Kyiv. Igor Sikorsky Kyiv Polytechnic Institute, 2020 – pp. 68 – 70. – ISSN(print)2663-502X.
6. Trubarov I.V. Design and Optimization of Coaxial-Fed Circular Patch Antenna for 2.4 GHz Frequency Band \ XIV International Scientific Conference "Modern Challenges in Telecommunications" MCT-2020. Conference proceedings. Kyiv. Igor Sikorsky Kyiv Polytechnic Institute, 2020 – pp. 74 – 76. – ISSN(print)2663-502X.

COUPLING COEFFICIENTS OF ROTATING RECTANGULAR DIELECTRIC RESONATORS IN CUT-OFF RECTANGULAR WAVEGUIDE

Trubin A. A.

*Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: atrubin9@gmail.com*

КОЕФІЦІЄНТИ ЗВ'ЯЗКУ ОБЕРТАЄМИХ ПРЯМОКУТНИХ ДІЕЛЕКТРИЧНИХ РЕЗОНАТОРІВ В ПОЗАМЕЖНОМУ ПРЯМОКУТНОМУ ХВИЛЕВОДІ

Досліджуються коефіцієнти взаємного зв'язку прямокутних діелектричних резонаторів, розташованих в позамежному прямокутному металевому хвилеводі при обертанні їх осей.

The rotation of the axes of dielectric resonators opens up additional possibilities for controlling the scattering parameters of various devices based on them [1-5]. The purpose of this report is to investigate mutual coupling coefficients of rotating rectangular DRs in the cut-off waveguide.

In this work, we calculated mutual coupling coefficients k_{12} of two identical rectangular dielectric resonators located in the cut-off waveguide with the possibility of rotation about one of the axes of the coordinate system (fig. 1, 2, a, d):

$$k_{12} = -k_{12}^0 \sum_{t=(0)}^{\infty} f_t^1(\mp i\Gamma) f_t^2(\pm i\Gamma)^* e^{-\Gamma \Delta z}.$$

Here k_{12}^0 - is the factor that depends only on the parameters of the resonators; t - multi index; Γ - longitudinal wave number of the cut-off waveguide; $\Delta z = |z_1 - z_2|$ - longitudinal distance between the centers of the resonators. The functions $f_t^s(\pm i\Gamma) = f_t^s(\pm i\Gamma; \alpha_s; \beta_s; \gamma_s)$ determine the dependence of the coupling on the angles of rotation $(\alpha_s; \beta_s)$ of the resonator relative to the waveguide ($s = 1, 2$).

We investigated the values of the maximum variation coupling coefficients when changing the angles of resonator rotation. The dimensions of the DR corresponded to the condition of excitation of the main magnetic oscillations in them H_{111} . The dielectric constant of each DR was assumed to be equal $\epsilon_{1r} = 36$; relative sizes $\Delta = L / a_0 = 0,4$; $B = b_0 / a_0 = 1$, where a_0 , b_0 - is the transverse dimensions, and L - is the height of the DR. The cross section of the rectangular waveguide was equal to $a \times b = 20 \times 15$ mm; H_{111} oscillation frequency $f_0 = 7$ GHz. Transverse coordinates of both resonators in the waveguide $x_{1,2} = a / 2$; $y_{1,2} = b / 2$.

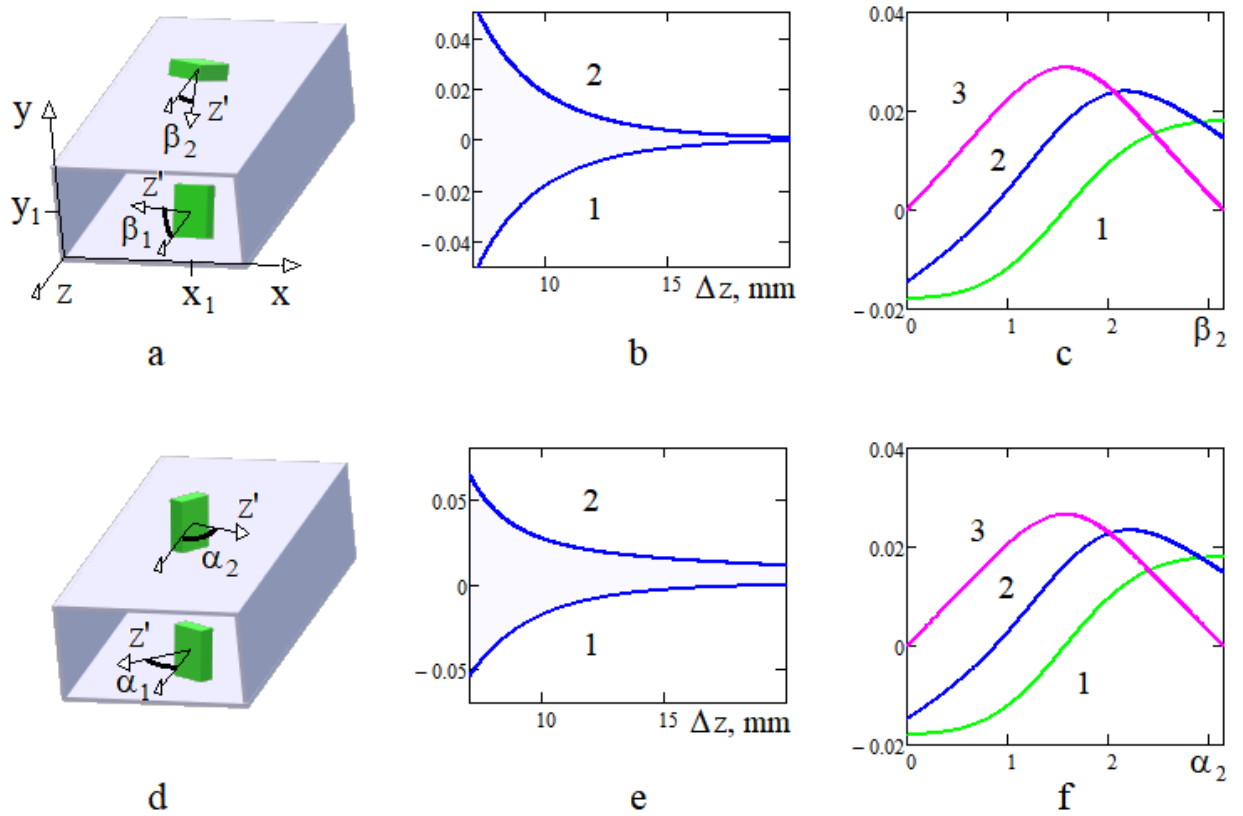


Fig. 1. Rectangular dielectric resonators rotating relatively the x (a) and y axis (d) in the rectangular waveguide. Variation of the mutual coupling coefficients at different longitudinal distances between the centers of rotating dielectric resonators in the waveguide (b (e)). Dependence of the mutual coupling coefficient on the angle of rotation of the second resonator.

Despite the fact that the functions $f_t^s(\pm i\Gamma)$ are complex, the mutual coupling coefficients in most cases remain real when the resonator axes rotate (see, for example, fig. 2, c).

In fig. 1, 2, b. e the dependences of the coupling coefficients on the longitudinal distance between the resonator centers are shown for $\alpha_1, \beta_1 = 0$ and $\alpha_2, \beta_2 = 0 - 1$; $\alpha_2, \beta_2 = \pi - 2$.

In fig. 1 and 2, c, f show the dependences of the coupling on the angle of rotation of the second resonator α_2, β_2 for $\alpha_1, \beta_1 = 0 - 1$; $\alpha_1, \beta_1 = \pi/4 - 2$; $\alpha_1, \beta_1 = \pi/2 - 3$ ($\Delta z = 10\text{mm}$).

As can be seen from the data obtained, the maximum variation of the coupling coefficients is determined by the distribution of the natural oscillation field of the resonators in the transverse plane (x', y') of local coordinate system. For natural oscillations of a rectangular DR H_{111} , the spatial distribution of the field is close to the dipole and uniform in the plane (x', y'), therefore, the rotation of the resonator in this plane has little effect on the coupling coefficients. A good example of this effect is the rotation of resonators about the longitudinal axis of the waveguide shown in Fig. 2, c.

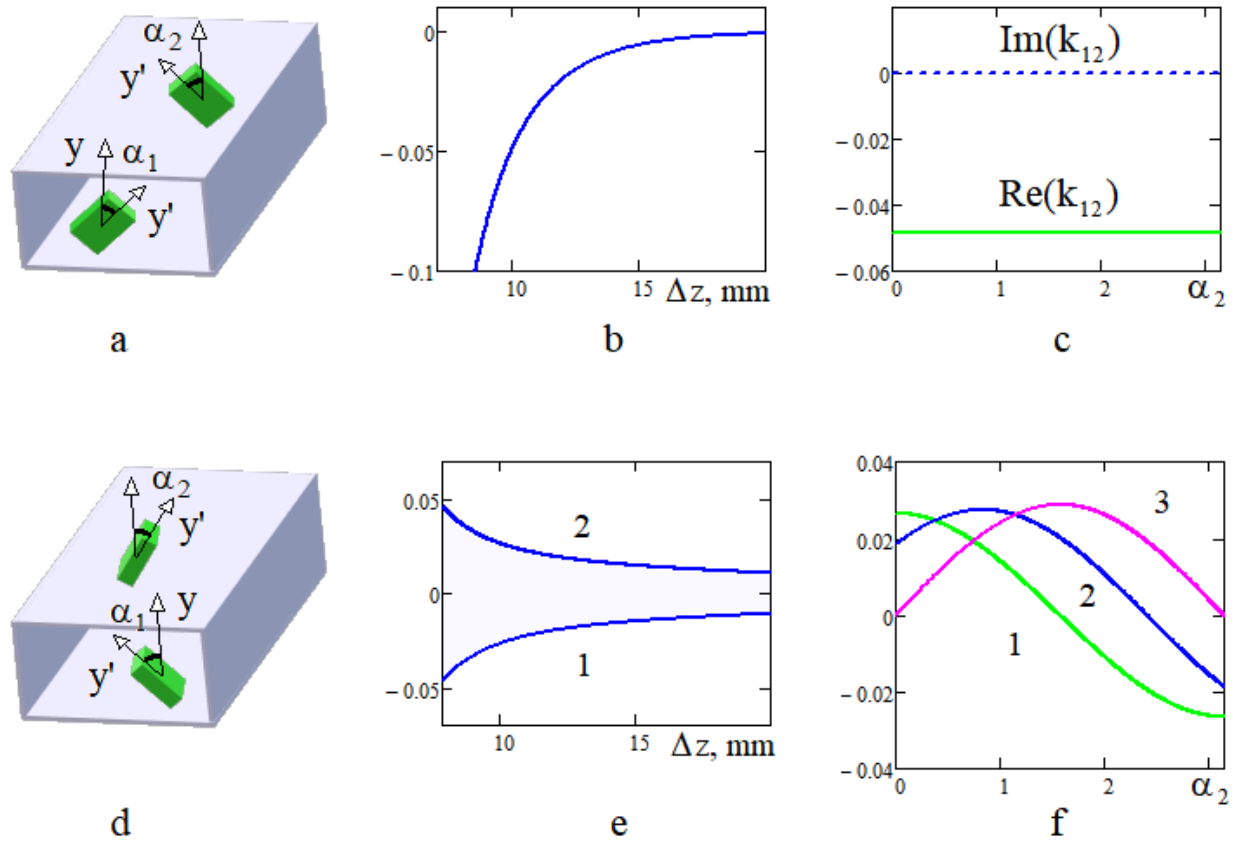


Fig. 2. Rectangular dielectric resonators rotating relative the z (a, d) axis for different initial positions in the waveguide. Variation of the mutual coupling coefficients at different longitudinal distances between the centers of rotating dielectric resonators in the waveguide (b, e). Dependence of the mutual coupling coefficient on the angle of rotation of the second resonator.

The obtained analytical relations for the mutual coupling coefficients make it possible to significantly expand the possibilities of designing and optimizing the parameters of wide range of band-pass and band-stop filters for microwave and millimeter-wave communication systems.

References

1. Fesenko V.I., Kupriianov A.S., Sherbinin A., Trubin A.A., Tuz V.R. All-dielectric Vogel metasurface antennas with bidirectional radiation pattern, *Journal of Optics*, UK, 22, 035104, 2020, pp. 1- 8.
2. Trubin A.A. Adaptive planar antennas on lattices of rotating Dielectric Resonators. 14 Int. Scientific Conf. Modern Challenges in Telecommunications. Kiev, 2020, pp. 89-91.
3. Shi T., Wang Y., Deng Z.-L., Ye X., Dai Z., Cao Y., Guan B.-O., Xiao S., Li X. All-Dielectric Kissing-Dimer Metagratings for Asymmetric High Diffraction // *Adv. Optical Mater.* WILEY-VCH Verlag, 2019, pp. 1901389 - 1901389.
4. Pidgurska T.V. Trubin A.A. Dual-bandpass filter built on rectangular dielectric resonators // *Radioelectronics and Communications Systems* / 2015. Vol. 58. PP.174–180.
5. Wang K., Titchener J. G., Kruk S.S., Xu L., Chung H.-P., Parry M., Kravchenko I. I., Chen Y.-H., Solntsev A. S., Kivshar Y. S., Neshev D. N., Sukhorukov A. A. Quantum metasurface for multi-photon interference and state reconstruction / *Science* vol. **361** (6407), pp. 1104-1108. <http://science.sciencemag.org/content/361/6407/1104>.

SCATTERING OF PLANE WAVES ON CUBIC SHAPE DIELECTRIC RESONATORS

Trubin A. A.

*Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: atrubin9@gmail.com*

РОЗСІЮВАННЯ ПЛОСКИХ ХВИЛЬ НА КУБІЧНИХ ДІЕЛЕКТРИЧНИХ РЕЗОНАТОРАХ

Досліджуються характеристики розсіювання у відкритому просторі електромагнітних хвиль на плоских решітках діелектричних резонаторів кубічної форми при збудженні основних вироджених магнітних типів коливань.

Lattices of rectangular dielectric resonators are actively studied as a basis for creating wide class of new devices [1-10]. Dielectric cubic resonators are more easily realized in optical integral devices, and also have a more rarefied spectrum of natural oscillations arising due to degeneracy. At the same time the presence of degeneracy significantly complicates the description of the behavior of lattices of cubic DRs in various structures. The development of the physical theory of scattering by complex structures of DRs [11, 12] made it possible not only to clarify their properties in various structures, but also showed the effectiveness of this approach to a unified method for describing various devices in the microwave and optical ranges. The purpose of this report is to calculation and analysis of field scattered by plain lattices of cubic DRs with lowest natural oscillations of magnetic type H_{111} .

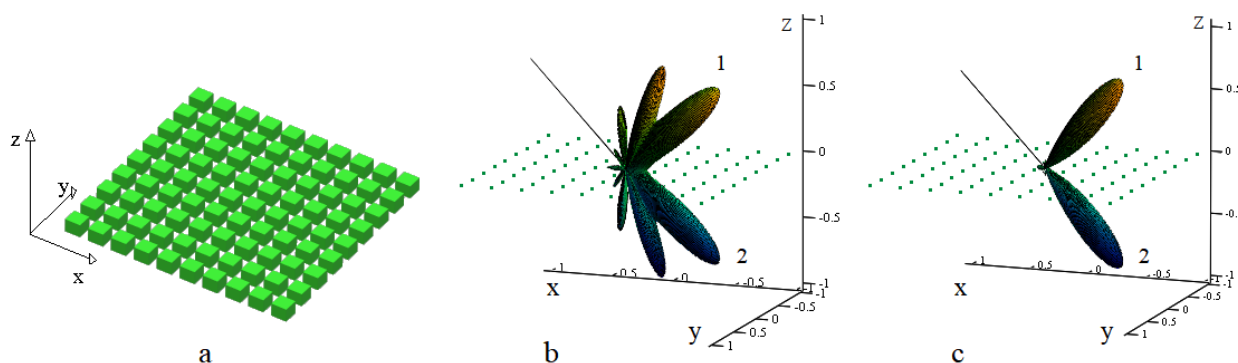


Fig. 1. A square lattice of a cubic shape DR (a). Angular distribution of the squared modulus of the scattering amplitude for a plane wave of the p-type (b), s-type (c) on the square lattice with H_{111} degenerate oscillations for $\vartheta_{\pi} = 3/4\pi$; $\varphi_{\pi} = 0$.

Relative dielectric constant of the resonators $\epsilon_{1r} = 36$.

To calculate the scattered field by the DR lattice, we used the perturbation theory [11]. The mutual coupling coefficients of cubic DRs were calculated by the formulas [12] taking into account the presence of a threefold degeneracy of each of the lattice resonators.

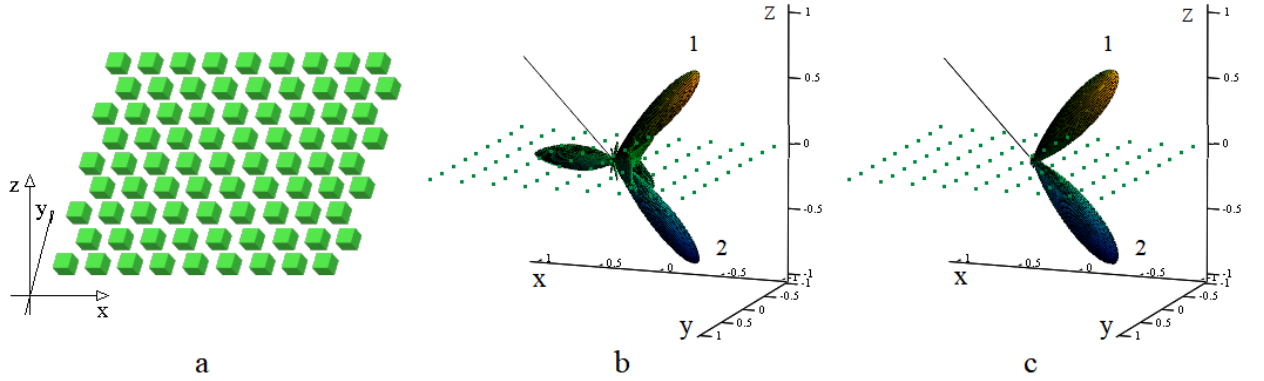


Fig. 2. A hexagonal lattice of a cubic DRs (a). The squared modulus of the scattering amplitude for a plane wave of the p-type (b), s-type (c) on the 10×10 cubic DR lattice ($\vartheta_\pi = 3/4\pi$; $\varphi_\pi = 0$; $\varepsilon_{1r} = 36$).

The scattering field of the lattice in the wave zone in the direction towards the observation point (θ, φ) represented as:

$$\vec{E}(\theta, \varphi) - \vec{E}^+(\theta_\pi, \varphi_\pi) = \vec{e}_0 f \langle \theta_\pi, \varphi_\pi | \theta, \varphi \rangle E_0 \frac{e^{-ik_0 r}}{k_0 r}, \quad (1)$$

where $(\vec{E}^+, \vec{H}^+)$ field of a plane wave incident on a lattice; $\vec{e}_0 = \vec{e}_0(\theta_\pi, \varphi_\pi | \theta, \varphi)$ - is the unit vector, defining the polarization of the scattered electric field in the wave-zone; $(\vartheta_\pi, \varphi_\pi)$ - is the incident wave direction in the spherical coordinate system of the lattice; $f \langle \theta_\pi, \varphi_\pi | \theta, \varphi \rangle$ is the scattering amplitude.

In fig. 1, 2, b, d shows the angular dependences of the squared modulus of the scattering amplitude for a plane p-type wave (b); s-type (c) on a lattice (a) of 10×10 DRs, respectively. The dots in (b, c) conventionally show the centers of the resonators; the straight line shows the direction of propagation of the incident wave $(\vec{E}^+, \vec{H}^+)$: $\vec{k}_0$. The relative distance between the centers of adjacent resonators is $\lambda_0/4$ (λ_0 is the wavelength in free space at the frequency of H_{111} resonant oscillations). As can be seen from the above data, petal 1 (fig. 2, b) is directed at an angle of "reflection" to the surface of the grating. Petal 2 is directed along the vector $\vec{k}_0$, whence, taking into account (1) and when the polarization of the incident and scattered waves coincides, it defines the lattice "shadow" resulting from reflection [11].

The emergence of a coupling between degenerate oscillations of cubic resonators can lead to the appearance of additional scattering lobes (fig. 1, 2, b).

Resonators in a hexagonal lattice are more weakly coupled to each other than in a cubic lattice; therefore, additional lobes in it are less noticeable. As can be seen from the data in Fig. 1, 2, b, additional lobes appear more often in the case of p-scattering. In this case, additional petals also lie in the plane of incidence.

The proposed theory can be used to calculate and analyze complex antenna structures, power dividers, filters, multiplexers, and other communication devices in the microwave, infrared and optical wavelength ranges.

References

1. Li J., Liu C., Wu T., Liu Y., Wang Y., Yu Z., Ye H., Yu L. Efficient Polarization Beam Splitter Based on All-Dielectric Metasurface in Visible Region, *Nanoscale Research Letters*. Springer Open, 2019, 14:34, <https://doi.org/10.1186/s11671-019-2867-4>, pp. 1 - 7.
2. Shi T., Wang Y., Zi-Lan Deng, Ye X., Dai Z., Cao Y., Bai-Ou Guan, Xiao S., Li X. All-Dielectric Kissing-Dimer Metagratings for Asymmetric High Diffraction. WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim, *Adv. Optical Mater.* 2019, 1901389, pp. 1 - 6.
3. Bibb L., Liu Q., Khan K., Yadav A., Elshahat S., Abood I., Ouyang Z.. Radiation-direction steerable nanoantennae // Research Article. Springer Nature, *SN Applied Sciences* (2019) 1:844 | <https://doi.org/10.1007/s42452-019-0882-9>.
4. Guo Z., Zhu L., Guo K., Shen F., Yin Z.. High-Order Dielectric Metasurfaces for High-Efficiency Polarization Beam Splitters and Optical Vortex Generators, *Nanoscale Research Letters*, Springer Open, 2017, 12:512, pp. 1 - 8.
5. Minin I. V., Minin O. V., Pacheco-Pena V., Beruete M. All-dielectric periodic terahertz waveguide using an array of coupled cuboids // *Applied physics letters*. Vol. 106, 254102, 2015, pp. 254102-1 - 254102-5.
6. Li L., Jun Wang, Jiafu Wang, Du H., Huang H., Zhang J., Qu S., Xu Z. All-dielectric metamaterial frequency selective surfaces based on high-permittivity ceramic resonators *Applied Physics Letters*, 2015, No 106, 212904, pp. 212904-1-5.
7. Petosa A., Thirakoune S.. Rectangular Dielectric Resonator Antennas With Enhanced Gain, *IEEE Trans. on Antennas and Propagation*, 2011, Vol. 59, No. 4, April, pp. 1385-1389.
8. Al-Zoubi A., Kishk A., Glisson A.W.. Linear dielectric resonator antenna array fed by dielectric image line. 2008 IEEE Antennas and Propagation Society International Symposium, San Diego, CA, USA, 2008, pp. 1 - 4.
9. Trubin A.A. Scattering of electromagnetic waves on a flat square lattice of cylindrical dielectric resonators // 19 International Crimean conference "Microwave equipment and telecommunication technologies". Sevastopol. 2009, pp. 405-407.
10. Mongia R. K., Ittipiboon A. Theoretical and Experimental Investigations on Rectangular Dielectric Resonator Antennas. *IEEE Trans. on Antennas and Propagation*, Vol. 45, No. 9, September 1997, pp. 1348 - 1356.
11. Trubin A.A. *Lattices of Dielectric Resonators*, Springer International Publishing Switzerland, – 2016 –, 171 p.
12. Trubin A. A., Kupriianov A.S., Fesenko V.I., Tuz V.R.. Coupling coefficients for dielectric cuboids located in free space // *Applied Optics*. OSA, 2020. Vol. 59, No 23/10, pp. 6918 - 6924.

Секція 3. Технології транспортних телекомунікаційних систем та мережні технології

УДК 621.39

ПОБУДОВА SDN-КОНТРОЛЕРА НА БАЗІ ВІДКРИТОЇ МЕРЕЖЕВОЇ ОПЕРАЦІЙНОЇ СИСТЕМИ ONOS

¹Корнієнко Н.І., ²Романов А.О.

¹*Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського*

²*Факультет аеронавігації, електроніки та телекомунікації НАУ*

E-mail: nkornienko2000@ukr.net, anton3329@gmail.com

BUILDING AN SDN CONTROLLER BASED ON THE OPEN NETWORK OPERATING SYSTEM (ONOS)

Possibilities, a list of control tasks and the main functional elements of an SDN controller based on ONOS are analyzed. Functional blocks that provide monitoring of networks and solutions to basic control problems are considered. It is shown that the implementation of ONOS simplifies the migration from traditional architecture to SDN.

ONOS (Open Network Operating System) – це відкрита мережева операційна система для управління SDN (Software Defined Networking) мережами і їх компонентами, такими як комутатори і канали, виконуючи програми або модулі для надання послуг зв'язку кінцевим хостам та сусіднім мережам [1]. Її особливість в тому, що вона поєднує в собі функціонал SDN-контролера, мережевої і серверної ОС. За рахунок такої комбінації інструмент дозволяє стежити за всім, що відбувається в мережах, і спрощує міграцію від традиційної архітектури до SDN [2].

ONOS був розроблений для задоволення потреб операторів, які бажають створювати рішення операторського класу, які використовують економіку напівпровідникового апаратного забезпечення для комерційних підприємств, пропонуючи гнучкість для створення і розгортання нових динамічних мережевих сервісів зі спрощеними програмними інтерфейсами. ONOS підтримує як налаштування, так і управління мережею в реальному часі, усуваючи необхідність запуску протоколів управління маршрутизацією і комутацією всередині мережевої структури. Перенесення інтелекту в хмарний контролер ONOS дозволяє впроваджувати інновації, і кінцеві користувачі можуть легко створювати нові мережеві додатки без необхідності змінювати системи передачі даних [4]. ONOS може працювати як розподілена система на декількох серверах, що дозволяє використовувати ресурси ЦП та пам'яті кількох серверів, забезпечуючи відмовостійкість у разі збою сервера і потенційно підтримуючи оновлення обладнання та програмного забезпечення в реальному часі або по черзі без переривання мережевого трафіку [3,4].

ONOS надає деякі, аналогічні серверним операційним системам, типи функцій, включаючи API-інтерфейси (Application programming interface) і абстракції, розподіл ресурсів і дозволу, а також програмне забезпечення, орієнтоване на користувача, таке як CLI (Command-line interface), GUI

(Graphical user interface) і системні програми. ONOS керує всією мережею, а не одним пристроєм, що може значно спростити управління, налаштування і розгортання нового програмного забезпечення, обладнання та послуг [3].

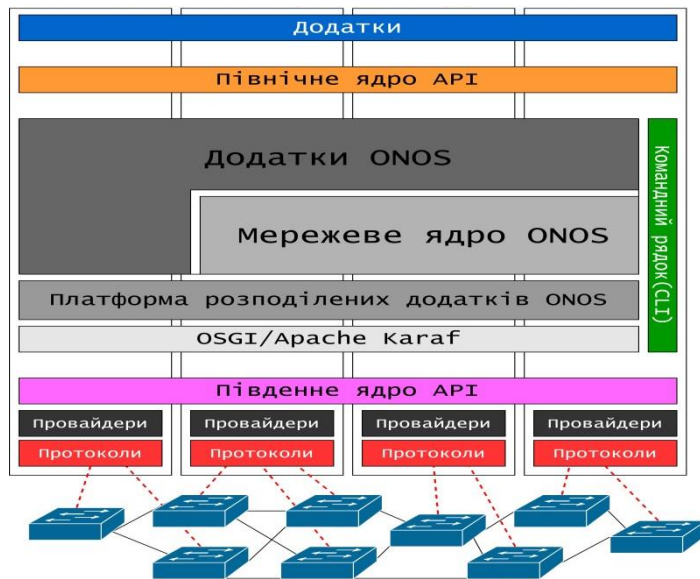


Рис.1. Розподілена архітектура ONOS.

Ядро ONOS і основні служби, а також додатки ONOS написані на Java у вигляді пакетів, які завантажуються в контейнер Karaf OSGi (Open Services Gateway initiative). Apache Karaf – це контейнер OSGi, що надає інфраструктуру для запуску OSGi-пакетів. OSGi – це компонентна система для Java, яка дозволяє встановлювати і запускати модулі динамічно в одній JVM (Java Virtual Machine). Оскільки ONOS працює в JVM, він може працювати на декількох базових платформах ОС.

Система призначена для роботи у вигляді кластера вузлів, які ідентичні з точки зору їх програмного стека і можуть витримувати відмову окремих вузлів, не викликаючи порушень в її здатності контролювати роботу мережі. Ядро ONOS відповідає за відстеження інформації про мережеве середовище і поширення його застосування або синхронно через запит, або асинхронно через слухаючі зворотні виклики. Ядро також відповідає за збереження стану вибору і синхронізацію стану між вузлами кластера. У ядрі відбувається основний логічний алгоритм. Цей блок забезпечує контроль станів, сповіщень, високу доступність та масштабованість.

Хоча ONOS в значній мірі спирається на стандартні протоколи і моделі, наприклад OpenFlow, який надає єдиний API, за допомогою якого адміністратори можуть програмувати роботу мережі, задавати правила маршрутизації пакетів, балансування навантаження і управління доступом. В ONOS є свій власний набір елементів і моделей високого рівня, який він надає розробникам додатків. Ці моделі можуть бути розширені додатками під час виконання. Щоб система не була прив'язана до певної конфігурації або протоколу керування, будь-яке програмне забезпечення, яке перебуває в прямому контакті з бібліотеками конкретних протоколів і бере участь в прямій взаємодії з мережевим середовищем. Платформа надає додаткам ряд високорівневих елементів, за допомогою яких додатки можуть дізнаватися про стан мережі і за допомогою яких вони можуть контролювати потік трафіку через мережу. Елементи мережевого графа надають інформацію про структуру і топології мережі.

Northbound (NB) API – північний інтерфейс та Southbound (SB) API – південний інтерфейс в ONOS налаштовані так, щоб додатки мали доступ до будь-якої інформації із будь-якої точки кластера. До Southbound API можна віднести такі протоколи як OpenFlow, Ethernet, SNMP (Simple Network Management Protocol), BGP (Border Gateway Protocol), OSPF (Open Shortest Path First) тощо.

Додатки ONOS виступають як розширення ядра, вони можуть бути бібліотеками протоколів, драйверами або попередньо скомпільованими моделями. Додатки можна завантажувати і вивантажувати динамічно, через REST API або графічний інтерфейс, і без необхідності перезапуску кластера або його окремих вузлів. REST (Representational State Transfer) – це популярний архітектурний підхід для створення API в сучасному світі. Відмінною особливістю сервісів REST є те, що вони дозволяють найкращим чином використовувати протокол HTTP (Hyper Text Transfer Protocol) – широко поширений протокол передачі даних, спочатку призначений для передачі гіпертекстових документів (тобто документів, які можуть містити посилання, що дозволяють організувати перехід до інших документів) [5,6].

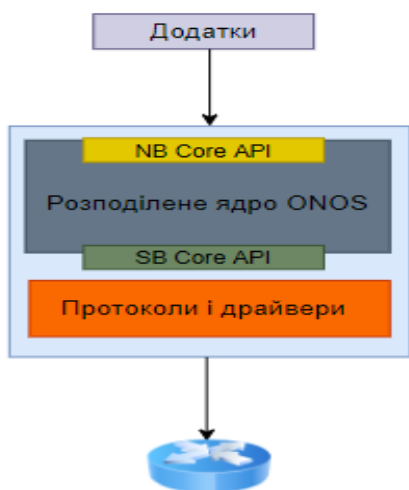


Рис.2. Принцип взаємодії елементів мережі SDN з контролером ONOS.

ONOS взаємодіє з наступними платформами та програмними елементами, що є зручним при переході від традиційних комп'ютерних мереж до SDN:

1. CORD, rCORD, mCORD, eCORD – платформа і варіанти центру обробки даних CO, використовувані в декількох областях: житлові, мобільні і міжмережеві з'єднання CO;
2. Packet-Optical – багатошарова мережа SDN, яка об'єднує пакетні і оптичні домени;
3. SDN-IP і VPLS (Virtual Private LAN Service) – SDN мережа як автономна система;
4. Сегментна маршрутизація – керована структура корінця-листка з високим ступенем використання і високої доступності.

Висновок. Стандартні служби ONOS дають можливість управління, моніторингу та маршрутизації програмно-конфігурованих мереж. ONOS працює як розподілена система, що забезпечує відмовостійкість у разі збою. Відкрита мережева операційна система є зручною платформою із відкритим вихідним кодом, що полегшує розробникам програмного забезпечення та обладнання у створенні технологій, які можна буде інтегрувати в SDN.

Література

1. Хабр. Как построить SDN — восемь инструментов с открытым исходным кодом [Електронний ресурс] / Блог компании VAS Experts. – 2019. – Режим доступу до ресурсу: <https://habr.com/ru/company/vasexperts/blog/446058/>.
2. O.I. Romanov, M.M. Nesterenko, N.O. Fesokha, V.B. Mankivskyi. Evaluation of productivity virtualization technologies of switching equipment telecommunications networks. Information and Telecommunication Sciences, 2020, Volume 11, Number 1 (20), p.53 – 58.
3. ONOS [Електронний ресурс] // Вільна енциклопедія «Вікіпедія». – 2020. – Режим доступу до ресурсу: <https://en.wikipedia.org/wiki/ONOS>.
4. ONOS: What is ONOS? [Електронний ресурс] // Open Network Operating System (ONOS) Wiki. – 2020. – Режим доступу до ресурсу: <https://wiki.onosproject.org/>.
5. О.І. Романов, М.М. Нестеренко, В.Б. Маньківський, І.О. Сайченко. Модель оптимального розподілу навантаження в мережі доступу мобільного оператора//Вісник ЧДТУ № 3 (2020), С.20-29.DOI: <https://doi.org/10.24025/2306-4412.3.2020>.
6. ONOS Overview [Електронний ресурс] // Open Networking Foundation – Режим доступу до ресурсу: <https://opennetworking.org/onos/>.

ДОСЛІДЖЕННЯ МЕРЕЖ SDN З ВИКОРИСТАННЯМ ПЛАТФОРМИ MININET

Романов О.І., Марінов А.І., Сколець С.С.

*Інститут телекомунікаційних систем КІП ім. Ігоря Сікорського, Україна
E-mail: a_i_romanov@ukr.net, marinov.anton99@gmail.com, serskols@gmail.com*

RESEARCH OF SDN NETWORKS USING THE MININET PLATFORM

Research of SDN networks using the programmable product Mininet. Creating and launching simulation network for research which based on Floodlight SDN Controller.

Мережа SDN є складною і дорогою системою. Зазвичай, після виконання етапу проектування мережі, необхідна тестова експлуатація з метою визначення показників функціонування та їх відповідність вимогам. Для цього використовуються різноманітні моделі: фізичні, аналітичні та імітаційні [1, 2].

Фізичні моделі припускають розгортання ділянки мережі на реальному обладнанні та його практичну експлуатацію з метою визначення характеристик функціонування. Цей метод дозволяє отримати дані, найбільш приближені до реальності. Однак такий підхід дуже дорогий та потребує великих затрат в часі. Тому цей метод застосовується нечасто.

Аналітичні моделі зручні в використанні і не потребують великих матеріальних затрат. Однак такі моделі тяжко отримати для таких складних систем, як телекомунікаційні системи. В них дуже низька точність і тому, часто неможливо математично описати модель, яка би відображала реальні процеси, які відбуваються у мережі.

Тому, як правило, використовують імітаційні моделі. Вони менш затратні, ніж фізичні моделі. При цьому вони дозволяють враховувати реальні процеси, які відбуваються у мережі та мають високу точність досліджуваних параметрів.

Для дослідження параметрів SDN мереж, організацією Open Networking Foundation (ONF) ведеться розробка платформи MININET. Елементи цієї платформи знаходяться в Інтернеті [3, 4]. Це дозволяє використовувати готові елементарні фрагменти для створення моделей SDN мереж різноманітної конфігурації. Варто відмітити, що моделі, які створені на платформі MININET, можуть не одразу запрацювати як слід. Та можуть вимагати певні зусилля в налагодженні. Однак, на сьогоднішній день платформа MININET достатньо зручна в роботі, має широкі можливості при створенні структур різної степені складності, а головне – вона знаходиться у вільному доступі.

Розглянемо принцип побудови моделі SDN мережі на базі мережевого емулятору Mininet [5, 6]. На рис.1 представлена структура мережі передачі даних, яка складається зі звичайних комутаторів та комп'ютерів. Ці елементи самостійно вирішують як задачі керування, так і задачі передачі даних.

Як що нам потрібно побудувати цю саму мережу на принципах SDN, необхідно провести розподіл і відділити площину контролю (control plane) від площини даних (data plane). При цьому за допомогою програмного продукту Mininet площину контролю над мережевим обладнанням буде перенесено до центрального SDN-контролеру. А площина даних залишиться на комутаторах. Крім того, ми будемо розглядати випадок, коли в ролі основного центрального керуючого елементу виступатиме Floodlight контролер.

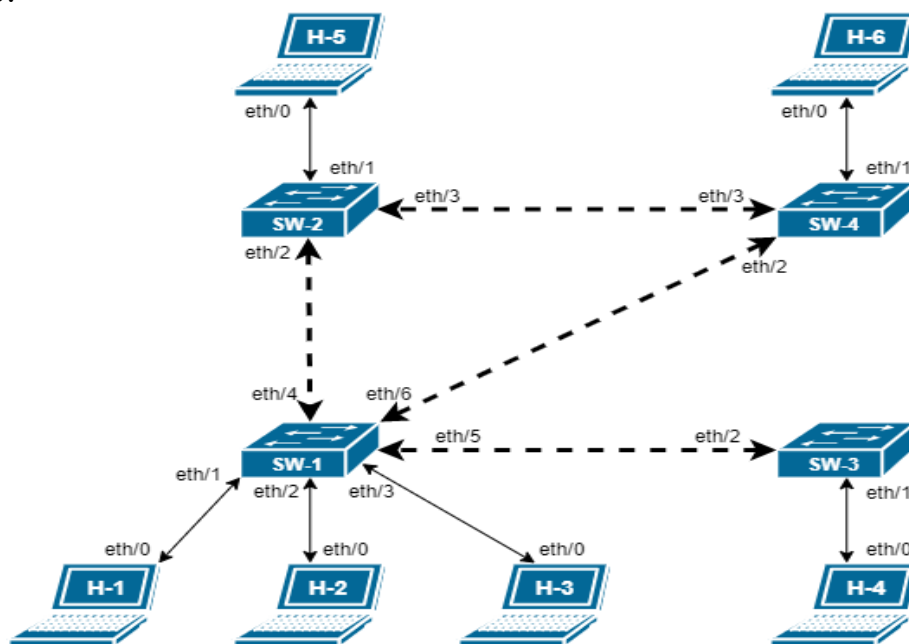


Рис.1. Структура фізичної мережі, яка буде перенесена в Mininet.

Взаємодія контролера з мережевими елементами забезпечується через “південний” інтерфейс з використанням стандартного відкритого протоколу OpenFlow. Цей стандарт підтримує організація ONF.

У ході виконання роботи необхідно використовувати програмний продукт VirtualBox для встановлення віртуальної операційної системи Linux Ubuntu. Це пов’язано з тим, що Mininet підтримує тільки Unix машини. Для управління елементами мережі в Mininet ми рекомендуємо використовувати контролер Floodlight тому, що цей контролер є в вільному доступі, являється академічним і активно розвивається. Треба враховувати, що установка мережі Mininet та контролера здійснюється на одній віртуальній машині [7, 8].

Перевагою такого принципу побудови моделі є те, що для створення і запуску лабораторного стенду знадобиться тільки власний персональний комп’ютер. Як вже раніше було зазначено, таку можливість надає Open Source-продукт Mininet, що знаходиться у вільному доступі. При цьому одночасно створюється віртуальна мережева топологія користувачських віртуальних OpenFlow-комутаторів і віртуальних хостів. Ці елементи керуються SDN-контролером. Фізична мережа рис.1 після перетворення у мережу SDN на базі платформи Mininet, буде набувати наступний вигляд рис.2.

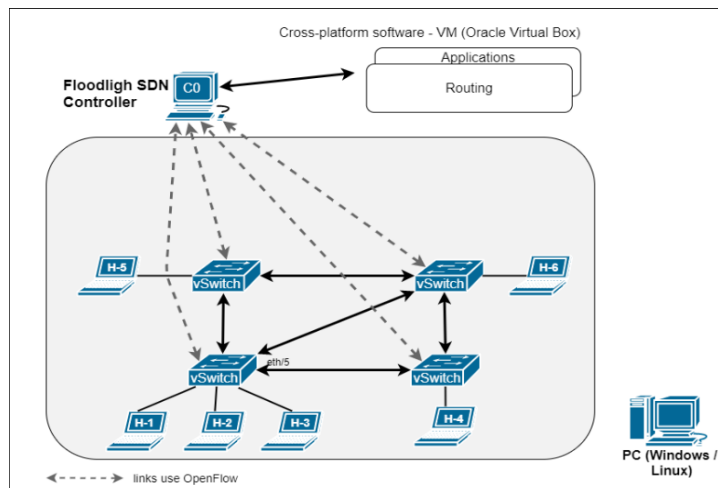


Рис. 2. Основні складові елементи досліджуваної SDN мережі у Mininet.

Дуже зручно, що при використанні Floodlight контролера є графічний web-інтерфейс. За допомогою web-інтерфейсу можна подивитися топологію мережі, дізнатися стан пристроїв у мережі, а також є можливість переглянути таблиці потоків на кожному віртуальному комутаторі (рис.3).

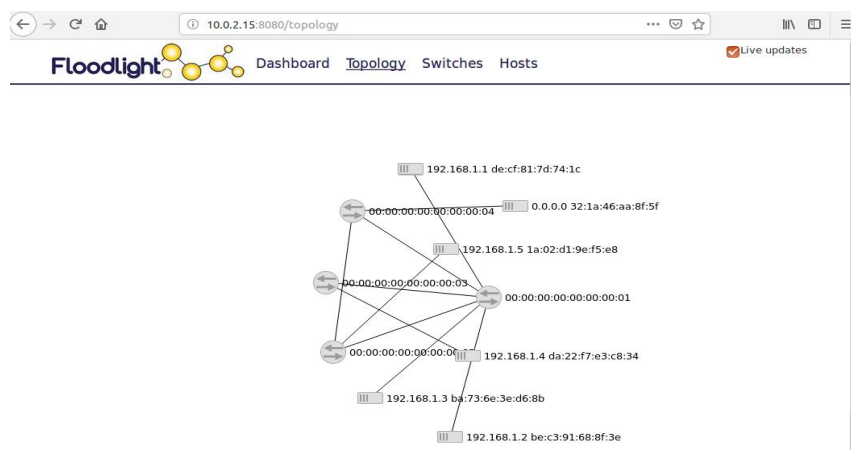


Рис.3. Візуальне відображення топології мережі в контролері.

Програмний продукт Mininet виділяється та приваблює тим, що він включає в себе ряд зручних елементів:

- команду лаунчера в терміналі (*mn*) для швидкого створення мереж; зручний Python API для створення мереж різного масштабу та різного типу топології;
- встановлені приклади реалізації функцій та різні типи топології;
- параметризовані топології (підклас Торо), використовуючи інтерфейс командної строки (CLI клас), який забезпечує корисні діагностичні команди типу: *iperf* та *ping*. Це також дає змогу запустити команди на кінцевому пристрої (хості);
- команда очищення (*cleanup*): *mn -c*, яка позбавляє, очищує операційну систему від непотрібних: інтерфейсів, процесів, файлів та інш., які можуть залишитися після роботи мережі Mininet та які обмежують здібності ОС. Наприклад: після зупинення мережі не було доступу до інтернету, поки не було прописано команду очищення: *mn -c*;

Після побудови та налаштування вищезазначеної мережі будуть виконані дослідження наступних параметрів в мережі:

- Пропускної здатності при навантаженнях каналів за допомогою UDP та TCP трафіку, що заодно дасть змогу перевірити Floodlight контролер на наявність можливості балансувати трафік при перенавантаженому каналі;
- RTT при різних значеннях затримки.

В основному для перевірок використовували інструмент iperf (для TCP протоколу) та iperfudp (для UDP протоколу), який в основному використовується для тестування пропускної здібності і базової оцінки продуктивності між мережевими елементами.

Для відстеження та отримання показників трафіку, використовується утиліта Wireshark. Яка може аналізувати мережеві пакети та по отриманим даним виводити та будувати графіки залежностей.

Хотілося б відмітити, що технологія SDN лише розвивається і поки що не має широкого впровадження. Проте ця технологія вважається дуже перспективною та вона дуже активно досліджується. І платформа Mininet дає змогу симулювати повноцінну роботу мережі з хостами, каналами зв'язку і контролерами. Знання та розуміння можливостей даної платформи, дозволяє досліджувати варіанти реальних мереж і зекономити кошти.

Література

1. C. Fancy and M. Pushpalatha, "Performance evaluation of SDN controllers POX and floodlight in mininet emulation environment," 2017 International Conference on Intelligent Sustainable Systems (ICISS), Palladam, India, 2017, pp. 695-699, doi: 10.1109/ISS1.2017.8389262;
- 2..Romanov O.I, Nesterenko M.M., Fesokha N.O., Mankivskyi V.B. Evaluation of productivity virtualization technologies of switching equipment telecommunications networks. Information and Telecommunication Sciences, 2020, Volume 11, Number 1 (20), page 53 – 58. DOI: <https://doi.org/10.20535/2411-2976.12020.53-58>
3. Lantz, Bob, Brandon Heller, and Nick McKeown. "A network in a laptop: rapid prototyping for software-defined networks." In Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks, pp. 19. ACM, 2010;
4. Nunes, B.; Mendonca, M.; Nguyen, X.; Obraczka, K.; Turletti, T., "A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks," Communications Surveys & Tutorials, IEEE, Vol. 1, No.99, pp. 18;
5. О.І. Романов, М.М. Нестеренко, В.Б. Маньківський, І.О. Сайченко Модель оптимального розподілу навантаження в мережі доступу мобільного оператора//Вісник Черкаського державного технологічного університету № 3 (2020), С.20-29, DOI: <https://doi.org/10.24025/2306-4412.3.2020>
6. Mininet official overview and walkthrough with commands here: <http://mininet.org/overview/> & <http://mininet.org/walkthrough/>;
7. Koerner (2012). "Multiple service load-balancing with openflow"., 2012 IEEE 13th international conference on In high performance switching and routing, pages 210-214, IEEE;
8. Скулиш, М. А., Романов О. І., Глоба Л. С. Принцип резервування ресурсів у віртуалізованому середовищі для контролю показників обслуговування // Вісник Інженерної академії України. – 2018. – С. 197-202. <https://ela.kpi.ua/handle/123456789/36912>

АНАЛІЗ ЕФЕКТИВНОСТІ ВИКОРСИТАННЯ TCP В МЕРЕЖАХ LTE

Маньківський В.Б., Педько А.Д.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

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

ANALYSIS OF THE EFFICIENCY OF TCP USE IN LTE NETWORKS

A feature of LTE is the presence of a wide range in the range of millimeter waves, which offers the ability to achieve speeds measured in megabits per second. However, the capacity of millimeter waves can be very intermittent due to the vulnerability of signals to blockages and delays in directional search. Such highly variable references present unique challenges for adaptive controls in transport layer protocols and end-to-end applications. This article discusses the key issue of how efficient the use of TCP, the most widely used transport protocol, is to work in cellular systems in the millimeter wave range. The paper offers a practical study of TCP taking into account various factors, such as congestion control algorithm, including the recently proposed TCP BBR, edge versus remote servers, handover and multi-connection, TCP packet size. We show that the efficiency of TCP on LTE references strongly depends on different parameters combinations.

Особливістю LTE є наявність широкого спектру в діапазоні частот, що пропонує можливість досягнути швидкості, яка вимірюється в мегабітах на секунду. Однак ємність частотного діапазону може бути дуже переривчастою через вразливість сигналів до завалів та затримок при спрямованому пошуку. Такі дуже мінливі посилення представляють унікальні виклики для адаптивних механізмів управління в протоколах транспортного рівня. У цій статті розглядається основне питання про те, яка ефективність використання TCP, найбільш широко використовуваний транспортний протокол, в стільникових системах LTE. У статті пропонується практичне дослідження TCP з урахуванням різних факторів, таких як алгоритм контролю перевантажень, включаючи нещодавно запропонований TCP BBR, віддалені сервери (MEC), хендовер та мульти-підключення, розмір пакета TCP. Ми показуємо, що ефективність TCP в LTE сильно залежить від різних комбінацій цих параметрів.

Якщо розглядати повний шлях підключення через Інтернет, то ми бачимо, що здебільшого передача покладається на транспортні протоколи, які працюють над мережевим рівнем. Найбільш широко використовуваним транспортним протоколом є Протокол управління передачею (TCP), розроблений у 1980-х роках [1], щоб запропонувати надійну доставку пакетів і контроль швидкості передачі, щоб запобігти перевантаженню мережі. Надійність досягається завдяки підтвердженням приймача (ACK), а контроль швидкості досягається динамічним регулюванням вікна перевантаження: максимальний обсяг даних, який відправник може передавати, не отримуючи ACK. Існує декілька алгоритмів контролю заторів (CC – Congestion Control) для покращення ефективності роботи та затримки TCP для різних типів мереж [2]. Однак, наступне покоління стільникових мереж представлятиме нові виклики для TCP, які демонструють нестабільну поведінку розповсюдження. Ця технологія розглядається як перспективний механізм

для цілей LTE - високої швидкості передачі даних та наднизької затримки [3], але наскрізна продуктивність, буде залежати від взаємодії з транспортними протоколами, такими як TCP. Деякі недавні дослідження [4, 5] підкреслювали, що надзвичайна мінливість якості сигналу дає погіршення пропускної здатності TCP, і дуже низьке використання ресурсів, або високу пропускну здатність за ціною високої затримки (за наявності повторних передач рівня зв'язку). Більше того, в [4] показано, що явище *bufferbloat* (тобто збільшення затримки, викликане надмірною буферизацією) виникає як наслідок присутності великих буферів у мережі. Наша мета – показати ефективність використання TCP в стільникових мережах з використанням LTE. Для досягнення цієї мети ми порівнюємо ефективність різних алгоритмів TCP CC на прикладі мережі LTE.

1. Передача даних та багатостороння підключеність: Через ненадійність окремих посилань міліметровими хвилями щільне розгортання невеликих комірок із протоколами швидкої передачі є критично важливими для підтримання стабільних зв'язків та уникнення таймаутів TCP.

2. Алгоритми CC: на віддалених серверах ми спостерігаємо більш високі варіації продуктивності різних алгоритмів CC, тоді як різниця майже незначна для граничних серверів. Загалом, вузьке місце TCP, пропускну здатність та зворотний шлях (BBR) перевершує TCP, що базується на втратах, як за швидкістю, так і за затримкою.

3. Розмір пакета TCP: Ми кількісно порівнюємо переваги передачі більших пакетів TCP у LTE та показуємо, що, враховуючи коливання швидкості передачі даних, розмір пакета забезпечує більш швидке зростання вікна перевантаження та вищу досягнуту швидкість.

Сценарій дослідження

Для того, щоб оцінити, як TCP буде працювати в стільникових мережах LTE, ми розглянемо один з найбільш повторювальний сценарій - місто.

В сценарії ми розглядаємо два сервера TCP, який діє як кінцева точка з'єднання. Перше - це традиційна установка, при якій сервер розміщується у віддаленому центрі обробки даних, з мінімальним часом зворотного зв'язку (RTT) близько 50 мс, враховуючи сукупну затримку: основної мережі і Інтернету. Другий - це сценарій мобільної хмарної хмари (MEC) [4], в якому сервер розташований недалеко від gNB з меншою затримкою (порядку 10 мс).

TCP congestion control algorithms

Ми вивчаємо чотири найбільш часто використовувані алгоритми CC.

TCP NewReno був алгоритмом за замовчуванням для більшості систем зв'язку. На фазі запобігання перевантаженню, потокова вікно перевантажень оновлюється після прийому кожного ACK. Оновлення базується на конструкції мультиплікативного зменшення (AIMD) з збільшенням добавки.

HighSpeed TCP призначений для мереж продукту із високою пропускну здатністю (BDP), в яких NewReno може демонструвати дуже повільний ріст потоку. HighSpeed поводить себе так само, як NewReno, коли *cwnd* малий, але коли він перевищує попередньо. Більше того, зростання вікон NewReno та HighSpeed залежить від швидкості прийому ACK; таким чином,

коротший RTT збільшує частоту АСК і додатково прискорює ріст вікна.

Натомість TCP CUBIC збільшує $cwnd$, не враховуючи швидкість прийому АСК, а скоріше фіксуючи абсолютний час з моменту останньої втрати пакету та використовуючи функцію кубічного збільшення для $cwnd$. Він був розроблений для збільшення швидкості нарощування кожного з'єднання, зберігаючи при цьому справедливість з іншими користувачами.

TCP BBR, нещодавно представлений Google [11], вимірює пропускну здатність вузького місця та час поширення в обидва кінці, або BBR, для здійснення контролю заторів. BBR для контролю заторів. Він прагне узгодити швидкість відправки з розрахунковою пропускну здатністю вузького місця шляхом стимуляції пакетів і встановлення вікна перевантаження на коефіцієнт посилення потоку BDP, де коефіцієнт посилення потоку є коефіцієнтом (≤ 2), який використовується для балансування ефектів затримки, розтягування та агреговані АСК для оцінки пропускну здатності.

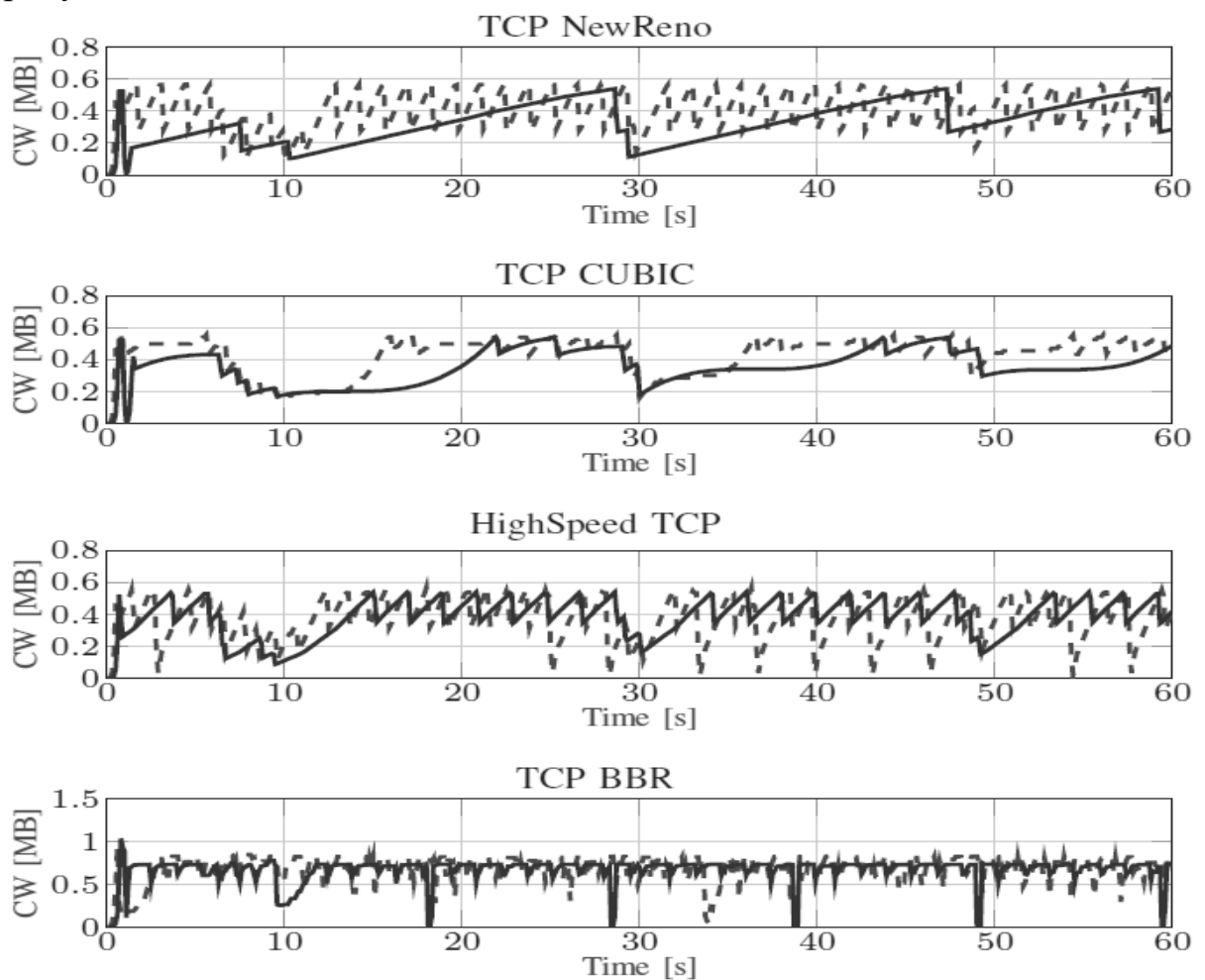


Рис. 1. Congestion Window (CW) with diff CC.

Impact of Congestion Control

Вплив алгоритму контролю заторів: алгоритм CC має сильніший вплив у сценарії віддаленого сервера. Найкращої продуктивності, з точки зору гарної продуктивності, досягає BBR з великим розміром буфера. Більше того, як зауважено в [4, 5], високі значення добротності також відповідають вищій

затримці. Однак при невеликих буферах BBR виробляє найвищу ефективність (особливо в сценарії крайового сервера), із затримкою, порівнянною з TCP на основі втрат. BBR, справді, регулює швидкість своєї передачі до розрахункової смуги пропускання і не позначається втратою пакетів, представленою на рис. 1. Однак версії TCP, що базуються на втратах, не можуть налаштувати своє вікно перевантаження настільки швидко, щоб адаптуватися до варіацій каналів і працювати гірше, ніж BBR, особливо з невеликим буфером, як показано на рис. 1. Серед них TCP HighSpeed забезпечує найвищу ефективність завдяки агресивному зростанню вікон у високій області BDP. TCP CUBIC працює краще, ніж NewReno, у випадку віддаленого сервера, але гірше у випадку крайнього сервера. Це пов'язано з тим, що зростання вікон CUBIC не впливає на швидкість АСК, а тому є надійнішим за довгих RTT-посилань.

Висновки. Велика, але переривчаста ємність, доступна на частотах LTE, створює нові проблеми для всіх рівнів стеку протоколів, включаючи TCP, найбільш широко використовуваний транспортний протокол. Взаємодія між алгоритмами контролю заторів та коливаннями якості каналу міліметрових хвиль робить тему особливо складною і представляє ключовий елемент цієї роботи. Основні висновки та деякі відповідні питання дослідження перелічені наступним чином:

- TCP виграє від коротшого циклу управління, де сервер розміщений на межі стільникової мережі і може швидше реагувати на порушення зв'язку.
- Більше того, коли RTT високий, TCP на основі втрат недостатньо використовує пропускну здатність міліметрових хвиль, тоді як ті, що базуються на перевантаженні (BBR), демонструють покращену продуктивність. Це означає, що нові підходи, засновані на більш вишуканих абстракціях наскрізної мережі, можуть бути вивчені для дуже змінних та високошвидкісних передачах.

Література

1. K. Liu and J. Y. Lee, "On Improving TCP Performance over Mobile Data Networks," IEEE Trans. Mobile Comp., vol. 15, no. 10, Oct. 2016, pp. 2522–36.
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. Mankivskiy Volodymyr and Pedko Andriy Concept of edge computing in mobile operator network // Modern challenges in telecommunications, vol. 14, 2020, pp. 51–54.
5. 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.
6. M. Xiao et al., Millimeter Wave Communications for Future Mobile Networks // IEEE JSAC, vol. 35, no. 9, Sept. 2017, pp.1909–35.
7. Oleksandr I. Romanov, Mykola M. Nesterenko, Nadiia O. Fesokha and Volodymyr B. Mankivskiy. Evaluation of productivity virtualization technologies of switching equipment telecommunications networks. // National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", 2020 - pp.: 132 – 138.

МОВА ПРОГРАМУВАННЯ P4 МЕРЕЖЕВИХ ПРИСТРОЇВ SDN

Нестеренко М.М., Топорков М.А.

Інститут телекомунікаційних систем КІП ім. Ігоря Сікорського, Україна

E-mail: nikolaiy.nesterenko@gmail.com, miha.toporkov@gmail.com

PROGRAMMING LANGUAGE P4 FOR NETWORK DEVICES SDN

Current trends in information technology place increasing demands on the flexibility and scalability of software-defined networks (SDN). These requirements contribute to the development of SDN management protocols. This paper discusses the P4 language, which can be an alternative to OpenFlow to describe packet processing in the switch.

Сучасні тенденції розвитку інформаційних технологій ставлять все більші вимоги до гнучкості та масштабованості програмно-конфігурованих мереж (SDN). Дані вимоги сприяють розвитку протоколів управління SDN. У цій роботі розглядаються характеристики мови P4 яка може спростити опис процесу обробки пакетів в комутаторі OpenFlow.

P4 - це мова програмування, призначений для програмування правил маршрутизації пакетів. Вона орієнтована на розробників, які описують принцип дії компіляторів, симуляторів і займаються налагодженням програм P4. На відміну від мови загального призначення, такого як C або Python, P4 - це предметно-орієнтована мова з рядом конструкцій, оптимізованих для мережевої маршрутизації.

Мова P4 з відкритим вихідним кодом, що ліцензується і підтримуваний некомерційною організацією, яка називається P4 Language Consortium. Вона також підтримується Open Networking Foundation (ONF) і Linux Foundation (LF) - двома найбільшими зонтичними організаціями в проектах з відкритим вихідним кодом в області мережеских технологій. Мова була придумана в 2013 році і описана в 2014 в документі SIGCOMM CCR під назвою «Programming Protocol-independent Packet Processors» [1]. З моменту свого створення P4 експоненціально зростає і розвивається, швидко стаючи стандартом опису передачі пакетів мережескими пристроями, включаючи мережескі адаптери, комутатори і маршрутизатори. «SDN перетворив мережеску індустрію, а P4 виводить SDN на новий рівень, забезпечуючи програмованість в області маршрутизації», - сказав Гуру Парулкар, виконавчий директор Open Networking Foundation.

Оскільки мова призначена для додатків маршрутизації, список вимог і варіантів дизайну відмінний порівняно з мовами програмування загального призначення. Основними рисами мови є:

1. Незалежність від цільової реалізації. Програми P4 розробляються так, щоб вони не залежали від реалізації, тобто вони можуть бути скомпільовані для безлічі різних типів виконавчих машин, таких як процесори загального призначення, FPGA, системи на кристалі, мережескі

процесори і ASIC. Ці різні типи машин відомі як цілі P4, і під кожен мету необхідний компілятор для перетворення вихідного коду P4 в модель цільового комутатора. Компілятор може бути вбудований в цільовий пристрій, зовнішнє програмне забезпечення або навіть хмарний сервіс. Оскільки багато з початкових цілей для програм P4 використовувалися для простої комутації пакетів, дуже часто можна почути термін «комутатор P4», навіть якщо вживання «ціль P4» найчіткіше.

2. Незалежність від використовуваного протоколу. P4 незалежний від протоколів. Це означає, що мова не має вбудованої підтримки поширених протоколів, таких як IP, Ethernet, TCP, VxLAN або MPLS. Замість цього програміст P4 описує формати заголовків і імена полів необхідних протоколів в програмі, які в свою чергу інтерпретуються і обробляються компільованою програмою і цільовим пристроєм.

3. Реконфігурованість полів. Незалежність від типу полів у заголовку пакетів. Модель абстрактної мови допускає реконфігурованість. Цілі P4 повинні мати можливість змінювати обробку пакетів після розгортання системи. Ця можливість традиційно пов'язана з маршрутизацією за допомогою процесорів загального призначення або мережевих процесорів, а не інтегральних схем з фіксованими функціями.

Процес програмування комутатору P4 зображено на рис. 1.

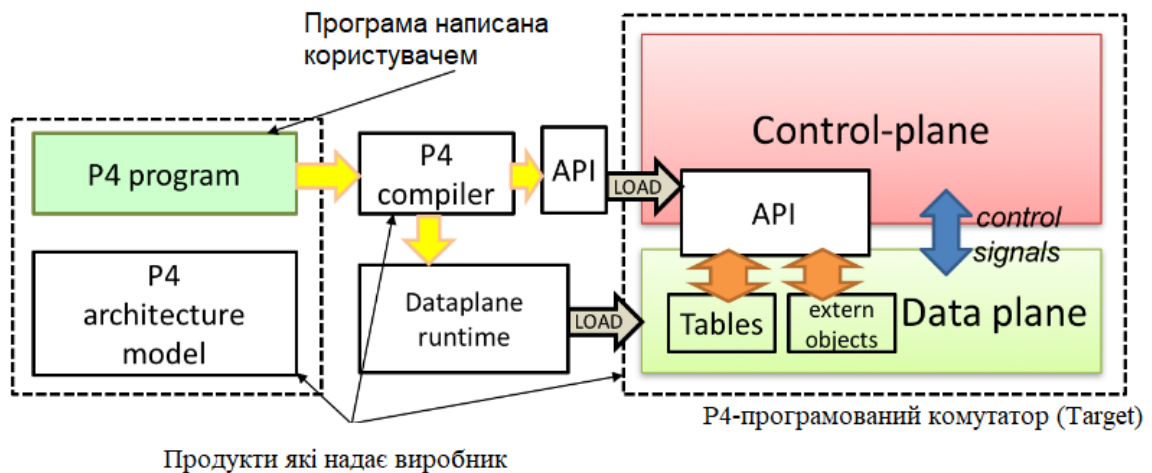


Рис. 1. Процес програмування комутатору P4.

Виробники комутаторів надають апаратну або програмну середовище реалізації, визначають архітектуру та компілятор P4 для реалізації певних задач на комутаторі. Програміст пише програму для конкретної архітектури, яка визначає набір програмованих P4 компонентів на машині, а також їх інтерфейси зовнішньої площини даних. Після чого компілятор генерує API, який потрібен для зв'язку площини управління з площиною даних. Та конфігурацію площини даних яка реалізує логіку пересилання пакетів описану в програмі P4.

Кожна програма P4 містить набір стандартних компонентів для опису обробки пакетів в площині даних:

- Заголовки - з їх допомогою визначаються заголовки протоколу. У

визначенні заголовків задаються опис форматів пакетів і імена полів заголовків та фіксовані і змінні дозволені поля.

- Парсери – завдання парсерів полягає в розбиванні пакету по заданим заголовкам.

- Таблиці - містять стани для пересилки пакетів, описують одиницю дії Match-Action.

- Дії - опис того, як слід маніпулювати пакетом. Дії складаються з коду і даних. Дані надходять управлінського рівня (наприклад, IP-адреси / номери портів). Певні, безциклові примітиви можуть бути задані безпосередньо в дії, але кількість команд повинно бути передбачуваним. Тому дії не можуть містити ніяких циклів або умовні оператори.

- Потік управління - вказує порядок застосування модулів Match-Action. Це імперативна програма, яка визначає логіку високого рівня і послідовність Match-Action. Потік управління пов'язує всі об'єкти, задаючи рівень управління.

На даний момент P4 знаходиться на початковій стадії прийняття, але він вже демонструє позитивну динаміку інтересу серед гравців ринку. Організації, що мають достатньо внутрішнього досвіду для програмування мережових чіпів, тепер можуть перетворити свої комутатори на все, що завгодно. Їм більше не потрібно чекати, поки їхній постачальник ASIC почне підтримувати новий протокол або змінить певний параметр, це можна зробити за допомогою внутрішніх інновацій.

Висновки. Ця гнучкість потенційно призводить до економічної ефективності, що дозволяє мережевим компаніям купувати апаратні компоненти безпосередньо у оригінальних виробників, не вдаючись до третьої сторони. Постачальники чіпів, у свою чергу, не хочуть допустити впровадження та навіть інвестувати в підтримку P4, щоб залишитися в тренді. Незважаючи на те, що невідомо, чи стане P4 галузевим стандартом, ініціативи таких компаній, як Google, Microsoft та інші, наближають його до такого.

Література

1. Pat Bosshart, Dan Daly, Martin Izzard, Nick McKeown, Jennifer Rexford, Cole Schlesinger, Dan Talayco, Amin Vahdat, George Varghese, David Walker, Programming Protocol-Independent Packet Processors. Barefoot Networks, Intel, Stanford University, Princeton University, Google, Microsoft Research. 2014.
2. Romanov O.I, Nesterenko M.M., Fesokha N.O., Mankivskyi V.B. Evaluation of productivity virtualization technologies of switching equipment telecommunications networks. Information and Telecommunication Sciences, 2020, Volume 11, N. 1 (20), page 53 – 58.
3. О.І. Романов, М.М. Нестеренко, В.Б. Маньківський, І.О. Сайченко «Модель оптимального розподілу навантаження в мережі доступу мобільного оператора»//Вісник Черкаського державного технологічного університету № 3 (2020), С.20-29.
4. <https://habr.com/ru/company/fgts/blog/460439/>.
5. <https://p4.org/p4-spec/docs/P4-16-v1.2.1.pdf>.
6. <https://github.com/p4lang>.

ДОСЛІДЖЕННЯ ПОКАЗНИКІВ ФУНКЦІОНУВАННЯ МЕРЕЖІ SDN З ВИКОРИСТАННЯМ MININET I FLOODLIGHT CONTROLLER

Романов О.І., Марінов А.І., Сколець С.С.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

*E-mail: a_i_romanov@ukr.net, marinov.anton99@gmail.com,
serskols@gmail.com*

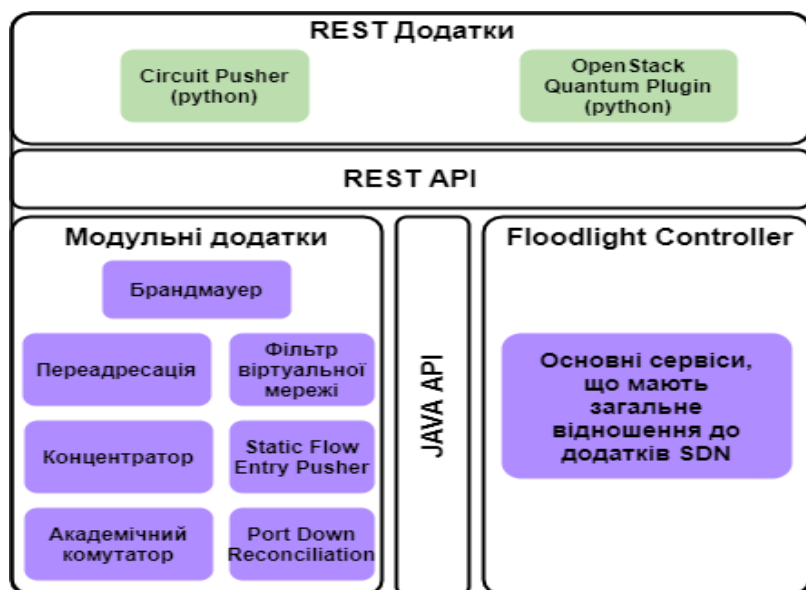
RESEARCH OF SDN PERFORMANCE USING MININET AND FLOODLIGHT CONTROLLER

Comparison of the results gained from the research of bandwidth in the transmission of TCP and UDP traffic, as well as checking for the availability of the balancing function on controller. Discovering and summarizing the results of the RTT research at the different values of delay in transmission channels. Summarizing the results of building a network on a Floodlight controller.

Floodlight Controller розроблений відкритою спільнотою розробників, які підтримують протокол OpenFlow. Моделювання мереж SDN на платформі Mininet з використанням Floodlight Controller має ряд переваг [1]:

- дає можливість легко адаптувати та розробляти програми, які написані на Java;
- включені інтерфейси прикладних програм REST API, які спрощують програмування інтерфейсу;
- веб-сайт Floodlight надає приклади кодування, які допомагають розробникам у створенні продукту;
- працює як з фізичними, так і віртуальними комутаторами, сумісними з OpenFlow;
- може підтримувати мережі на традиційних комутаторах, які не є OpenFlow.

Структура і основні функціональні елементи Floodlight Controller представлені на рис 1.



* Модульні додатки - додатки з вищою пропускну здібністю для комунікації з контролером, такі як Packin's

Рис. 1. Функціональна структура контролеру.

Розглянемо призначення основних елементів, REST додатки – програми на будь-якій мові, що використовують сервіси за допомогою REST API, що керуються модулями контролера та модульними додатками [2, 3]. Розглянемо призначення основних елементів, REST додатки

– програми на будь-якій мові, що використовують сервіси за допомогою REST API, що керуються модулями контролера та модульними додатками [2, 3]. Контролер Floodlight (рис.1) сумісний з OpenStack набором програмних інструментів, які дають можливість створювати та керувати платформами хмарних обчислень для загально користувацьких та приватних хмар. Floodlight можна запустити як мережевий сервер для OpenStack. Плагін Neutron надає модель мережі.

Circuit Pusher з REST API забезпечує управління потоками пакетів на всіх комутаторах на основі IP-адрес із заданим пріоритетом.

Брандмауер - програма для застосування правил ACL для дозволу / заборони трафіку на основі вказаного збігу (відповідності). Переадресація – програма переадресації пакетів Floodlight за замовчуванням. Концентратор – програма-концентратор, яка завжди пересилає всі вхідні пакети на всі інші активні порти. Навчальний комутатор – типовий комутатор рівня L2. Виставляє REST API для таблиці комутаторів (відомі хости: vlan: порт). Фільтр віртуальної мережі – простий додаток для ізоляції мережі на основі MAC. Виставляє набір REST API для додавання, видалення та запитування віртуальних мереж. Static Flow Entry Pusher – додаток для встановлення конкретного входу потоку (співвідношення + дія) на певний комутатор. Виставляє набір REST API для додавання, видалення та запиту записів потоку. Port Down Reconciliation – додаток для узгодження потоків через мережу, коли порт або посилення перестають працювати.

В роботі на базі використання Mininet і Floodlight Controller були досліджені наступні параметри мережі:

- Пропускна здатність каналів мережі при передаванні пакетів UDP та TCP трафіку;
- балансування трафіку Floodlight контролером в режимі перевантаження каналів;
- затримка пакетів RTT при різному навантаженні каналів.

При дослідженні пропускної здатності по каналах велася передача пакетів UDP та TCP з використанням інструментів iperf (для TCP протоколу) та iperfudp (для UDP протоколу).

Таблиця 1. Результати дослідження пропускної здатності

Відрізок передачі	Задане навантаження	Експериментальне навантаження	Розмір переданого трафіку	Середня затримка пакетів	Кількість переданих/втрачених пакетів
Від H1 до H5	6 Мбіт/с	3.7 Мбіт/с	14 МБ	18.621 мс	15201/5238 (34% втрат)
Від H3 до H5	4 Мбіт/с	2.4 Мбіт/с	9.03 МБ	1.787 мс	10178/3741 (37% втрат)
Від H4 до H5	5 Мбіт/с	2.97 Мбіт/с	11 МБ	1.683 мс	12674/4847 (38% втрат)

В цьому експерименті ми використовували 5-й вузол (Host 5) у якості серверу який приймає трафік від трьох клієнтів, якими є 1-й, 3-й та 4-й вузли (відповідно Host 1, Host 3, Host 4). При первинному налаштуванні пропускна здатність усіх каналів в мережі було встановлено 10 Mbit/s. Далі було створено навантаження для кожного клієнта так, щоб було наявне перевантаження. Наприклад, гілка мережі має пропускну здатність 10 Mbit/s, а сумарне навантаження складає 15 Mbit/s. Тобто ціль в тому щоб трафік не пішов по одному найкоротшому шляху, а потрібно було його балансування. В нас частина відправлених пакетів розподілилась на відрізок передачі від sw-1 до sw-4, щоб запобігти появі втрат на відрізок передачі від sw-1 до sw-2. Отримані результати наведені в таблиці 1. Візуально процес перевантаження зображений на рис. 3.

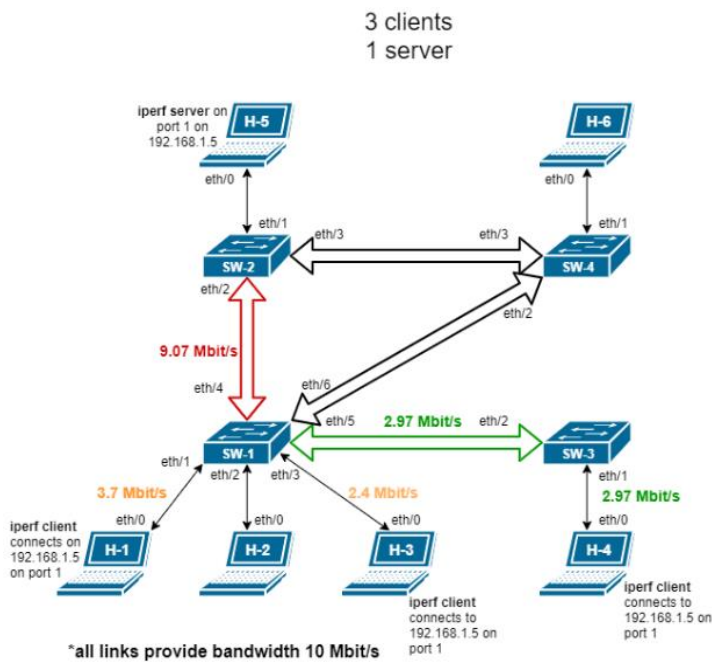


Рис. 3. Процес перенавантаження каналу зв'язку в досліджуваній мережі.

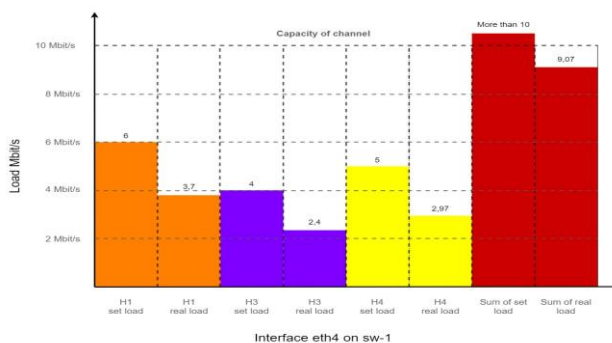


Рис.4. Навантаження на інтерфейсі eth4 комутатора sw-1.

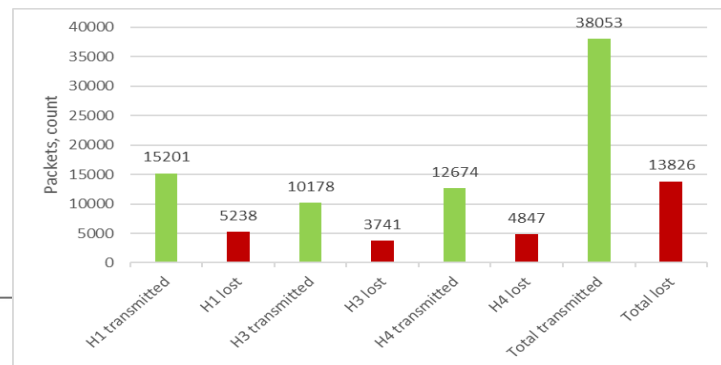


Рис. 5 Статистика передачі пакетів між клієнтами та сервером

За визначення параметру RTT відповідає команда *pingall*. Але для отримання більш розгорнутої статистики використовують команду: *pingallfull*.

Результати дослідження RTT наведені в табл.2.

Таблиця 2. Результати дослідження RTT.

Затримка, мс	Середній RTT, мс	Кількість робочих напрямків зв'язку	Кількість відказаних відрізків
0	0.146	30	0
2.5	22.266	30	0
5	38.578	30	0
50	308.414	30	0
100	909.721	30	0
200	1792.005	30	0
400	3358.825	28	2
450	3693.478	27	3
500	3131.509	18	12

Візуалізація отриманих результатів представлено на рис.6 і рис.7.

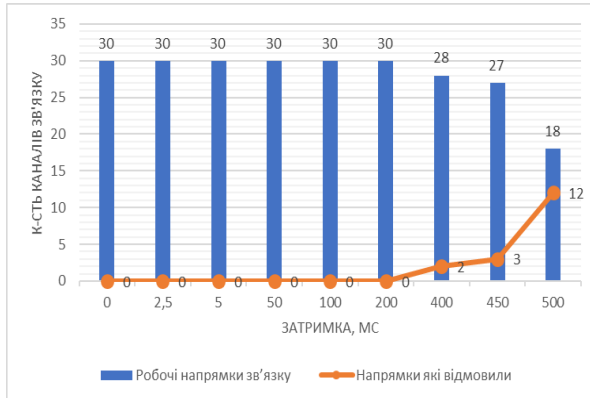


Рис. 6. Залежність кількості робочих і відмовлених напрямків зв'язку при різних затримках в мережі.

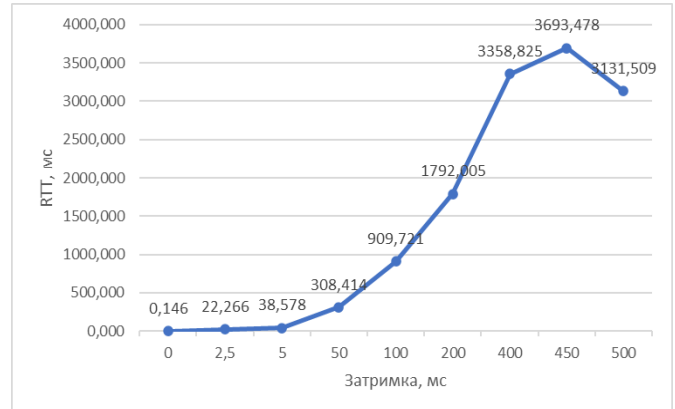


Рис. 7. Залежність зміни RTT при різних затримках в мережі.

Як видно з рис 6, коли передаються пакети зі встановленою затримкою в мережі 400 мс, починають відбуватися перші відключення напрямків зв'язку. А саме відмовляють 2 напрямки з найбільшою кількістю хопів, при 30-ти напрямках зв'язку в мережі (де хоп це «відстань» між двома вузлами в мережі, тобто чим більше хопів — тим складніший шлях маршрутизації і тим «далі» знаходяться вузли один від одного).

Відповідно на рис 7, можна спостерігати спад RTT при затримці 450 мс, що обумовлено відмовою 3-х каналів. При затримці в 500 мс, бачимо набагато більшу кількість відмовлених, а саме 12 напрямків зв'язку.

Також, в результаті проведення дослідів при встановленні всіх вищезазначених затримок (табл. 2), нами були помічені лінії зв'язку з найбільшими затримками: h1-h4, h1-h5, h1-h6, h2-h4, h2-h5, h2-h6, h3-h4, h3-h5, h3-h6, h4-h5, h4-h6, h5-h4, h5-h6, h6-h4.

Таким чином, використання Mininet дозволяє моделювати достатньо складні мережі SDN і отримати важливі показники їх функціонування, такі як пропускна здатність, якість обслуговування, затримка пакетів з використанням різних протоколів, наприклад TCP, UDP та інші. Mininet є у відкритому доступі. Тому вона заслуговує більш детального вивчення.

Література

1. C. Fancy and M. Pushpalatha, "Performance evaluation of SDN controllers POX and floodlight in mininet emulation environment," 2017 International Conference on Intelligent Sustainable Systems (ICISS), Palladam, India, 2017, pp. 695-699, doi: 10.1109/ISS1.2017.8389262;
2. О.І. Романов, М.М. Нестеренко, В.Б. Маньківський, І.О. Сайченко Модель оптимального розподілу навантаження в мережі доступу мобільного оператора//Вісник Черкаського державного технологічного університету № 3 (2020), С.20-29, DOI: <https://doi.org/10.24025/2306-4412.3.2020>
3. Lantz, Bob, Brandon Heller, and Nick McKeown. "A network in a laptop: rapid prototyping for software-defined networks." In Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks, pp. 19. ACM, 2010;
4. Romanov O.I, Nesterenko M.M., Fesokha N.O., Mankivskyi V.B. Evaluation of productivity virtualization technologies of switching equipment telecommunications networks. Information and Telecommunication Sciences, 2020, Volume 11, N 1 (20), page 53 – 58.

ПИТАННЯ ВПРОВАДЖЕННЯ СТАНДАРТУ 5G НА БАЗІ ІСНУЮЧОЇ ІНФРАСТРУКТУРИ МЕРЕЖІ

Тріска Н.Р.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: ntriska@ukr.net

THE ISSUES OF 5G DEPLOYMENT BASED ON THE LEGACY NETWORK INFRASTRUCTURE

The first experience of 5G deployment on the typical mobile operator networks is analyzed. The problems of adaptation of the legacy network infrastructure for 5G requirements are considered, especially in the field of network synchronization.

В доповіді проаналізовано перший практичний досвід впровадження стандарту 5G на існуючих мережах операторів мобільного зв'язку. Розглядаються проблеми адаптації існуючої мережевої інфраструктури до вимог 5G, зокрема. в частині забезпечення синхронізації.

Однією з провідних тенденцій розвитку сучасних інфокомунікацій є впровадження нового стандарту мобільного зв'язку (5G). Мережа 5G, основними засадами якої є суттєве збільшення швидкості передавання даних та впровадження програмно-конфігурованої архітектури з віртуалізацією мережевих функцій (SDN/NVF), стала базовою концепцією розвитку інформаційно-комунікаційних технологій на найближче десятиріччя.

Протягом останніх років основну увагу телекомунікаційної спільноти було спрямовано на розробку та стандартизацію загальних положень та технічних рішень для майбутніх мереж 5G, і в цьому напрямку досягнуто значного прогресу [1, 2]. Основний обсяг технічних специфікацій для майбутніх мереж 5G розробляється в рамках Партнерського проекту 3GPP (3rd Generation Partnership Project). Координацію діяльності з міжнародної стандартизації технології 5G здійснює Міжнародний Союз Електрозв'язку ITU-T в рамках платформи IMT-2020. Ці процеси будуть тривати і надалі, оскільки велике коло питань потребує детальних досліджень і опрацювання. Але наразі на перший план виходять практичні аспекти впровадження розроблених стандартів на реальних мережах.

В багатьох країнах світу (у Великобританії, Японії тощо) провідні телекомунікаційні оператори вже почали будівництво мереж 5G, вирішуючи питання адаптації існуючої мережевої інфраструктури до технічних вимог стандартів 5G. Незважаючи на значну кількість напрацьованих нормативних документів, важко переоцінити роль практичного досвіду дослідної та комерційної експлуатації нових мереж 5G, оскільки такий досвід дозволяє виявити сильні та слабкі сторони запропонованих технічних рішень і знайти оптимальні шляхи впровадження нової технології з максимальним використанням існуючої інфраструктури.

Розглянемо деякі аспекти впровадження стандарту 5G на основі досвіду провідних операторів [3, 4].

Дослідне розгортання мереж 5G виявляє нездатність мереж попередніх технологій задовольнити вимоги 5G – як в частині доступу (за визначенням), так і в частині базової ТМ з забезпечення зростання пропускну здатності.

Розвиток мереж мобільного зв'язку демонструє стабільну тенденцію зростання ролі синхронізації і, відповідно, збільшення кількості використовуваних методів та технічних засобів і встановлення більш жорстких нормативних вимог до точності частоти та/або фази. В таблиці 1 наведено основні показники різних стандартів мобільного зв'язку – від 1G до 5G (зокрема, вимоги до точності частоти та фази на базових станціях). Необхідність в точній синхронізації виникла на етапі впровадження мереж стандарту 2G (GSM), що спиралися на транспортну інфраструктуру SDH. На той час мова йшла лише про тактову (частотну) синхронізацію. Але з появою стандарту 3G (технологія з кодовим розділенням каналів – CDMA) окрім частотної синхронізації знадобилася також синхронізація фази/часу, що було пов'язано з впровадженням нових послуг (локації, “м'якого” передавання обслуговування – handover, тощо). Ці тенденції набули подальшого розвитку на етапі впровадження стандарту 4G (на базі технології розділення ортогональних несучих – OFDMA) і залишаються актуальними під час розгортання мереж 5G. Більше того, забезпечення точної фазової синхронізації на кожній базовій станції (БС) є необхідною умовою виконання жорстких вимог стандарту 5G щодо низької затримки передавання даних (порядку 1 мс, на відміну від 10 мс в системах 4G).

Таблиця 1. Основні показники стандартів мобільного зв'язку.

1G ⇒	2G ⇒	3G ⇒	4G ⇒	5G
1980 р.	1990 р.	2000 р.	2010 р.	2020 р.
ДОСТУП ↓				Концепція IMT-2020/5G
FDMA	TDMA	CDMA	OFDMA	
ПОСЛУГА ↓				
АМ	ЦМ, ПД, 2-3 кб/с	ЦМ, ПД: ~ 20 Мб/с	ЦМ ПД: 100 Мб/с~1Гб/с	
ТАКТОВА (ЧАСТОТНА) СИНХРОНІЗАЦІЯ ↓				
ні	так	так	так	так
	$\pm 5 \cdot 10^{-8}$	$\pm 5 \cdot 10^{-8}$	$\pm 5 \cdot 10^{-8}$	$\pm 5 \cdot 10^{-8}$
ФАЗОВА / ЧАСОВА СИНХРОНІЗАЦІЯ ↓				
ні	ні	так	так	так
		$\pm 1,25$ мкс/TDD	± 1 мкс/TDD; $\pm 0,5$ мс/FDD	$\pm 1,5$ мкс
АМ – аналогова мова; ЦМ – цифрова мова; ПД – передавання даних				

В стандартах 3G фазова синхронізація була потрібна лише в разі використання систем з часовим розподілом напрямків передавання – TDD (Time Division Duplex). Але часто оператори використовували варіант з частотним розподілом напрямків – FDD (Frequency Division Duplex), де було достатньо добре відпрацьованих технічних рішень з частотної синхронізації. З впровадженням 4G і особливо 5G постала необхідність забезпечення на кожній БС фазової синхронізації з точністю не гірше $\pm 1,5$ мкс, що іноді важко реалізувати на базі існуючого обладнання (або навіть неможливо, особливо з огляду на перспективу впровадження ще більш жорстких вимог –

точності порядку ± 260 нс). Кожний оператор вирішує цю проблему виходячи зі своїх технічних та фінансових можливостей, і дуже важливо знайти оптимальні варіанти впровадження нових технічних рішень з фазової/часової синхронізації.

На фрагментах мережі, де створюється повністю нова транспортна інфраструктура, адаптована до вимог 5G, технічних проблем з забезпеченням фазової синхронізації не виникає. Але на “старих” фрагментах треба шукати оптимальні рішення. Одним з таких компромісних варіантів, що може використовуватись під час “перехідного періоду”, є використання подвійного підключення – ENDC (E-UTRAN New Radio - Dual Connectivity), яке дозволяє надавати користувачу окремі функції 5G до створення повноцінної транспортної інфраструктури 5G із забезпеченням фазової синхронізації. Технологія ENDC дозволяє підключати абонентський термінал одночасно до мереж 4G та 5G з обміном даними між ними (в тому числі в частині синхронізації). Це дозволяє використовувати фазову синхронізацію з існуючої мережі 4G (FDD) з точністю $\pm 0,5$ мс.

Також можливе вирішення проблеми фазової синхронізації на локальному рівні – шляхом встановлення приймача GPS на кожній БС, що потребує синхронізації. Але таке рішення має бути технічно можливим і економічно обґрунтованим.

В даних тезах висвітлено лише окремі питання впровадження 5G, але подібні обмеження та необхідність пошуку компромісних варіантів стосуються не лише забезпечення синхронізації, а й інших аспектів впровадження.

Можна констатувати, що для подальшого розвитку сценаріїв розгортання та введення в комерційну експлуатацію мереж 5G необхідне аналітичне опрацювання набутого досвіду перших пілотних проектів. Під час розгортання мереж 5G необхідно враховувати той факт, що ці пілотні проекти частково реалізуються на базі існуючої інфраструктури, яка створювалася для підтримки стандартів мобільного зв'язку попередніх поколінь (2G/3G/4G) і наразі продовжує виконувати ці функції. Але практика впровадження вказує на неможливість перманентного розвитку від 4G до 5G. Тому планування та проведення дослідної експлуатації потребує ретельного дослідження технічних умов та засобів реалізації мереж 5G.

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. Тріска Н.Р. Синхронизация в телекоммуникациях нового поколения: обзор технологий и стандартов. – Дванадцята Міжнародна науково-технічна конференція “Проблеми телекомунікацій” (ПТ-2018), 16-20 квітня 2018 р. Матеріали конференції. – ІТС НТУУ “КПІ”. – С. 101-103.
3. M. Kingston. Deploying Phase Synchronisation. When strategy met reality. – The International Timing and Sync Forum (ITSF), 1-4 November 2020.
4. S. Ruffini, M. Johansson, B. Pohlman, M. Sandgren 5G synchronization requirements and solutions. – Ericsson technology review, January 2021. – p. 2-13.

ПІДВИЩЕННЯ НАДІЙНОСТІ ФУНКЦІОНУВАННЯ МЕРЕЖ SDN МЕТОДОМ РЕЗЕРВУВАННЯ КОНТРОЛЕРІВ

Атаманчук М.В., Сайченко І.О.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: atamanchuk14kolya@gmail.com, paramayson@gmail.com

IMPROVING THE RELIABILITY OF SDN NETWORKS BY BACKING UP CONTROLLERS

One of the features of building SDN networks is the presence of a network controller. The controller is the only point of failure of which will lead to the failure of the entire network. The paper considers the system for improving the fault tolerance of the DISCO network and proposes the creation of a common database for redundancy and replication of the controller settings to other elements of the control network.

Інформаційні технології сьогодення висувають все більше вимог до гнучкості та масштабованості мереж. Саме з цієї причини й виникла потреба у створенні мережі нового покоління. Такою мережею стали програмно-конфігуруючи мережі SDN. Програмно-конфігуруючи мережі мають унікальну відмінність від всіх інших, SDN має свій власний мозок який називається контролером мережі. Контролеру випала роль керувати всією структурою мережі, та мати доступ до кожного з її елементів.

Контролер SDN являє собою єдину точку відмови, що робить архітектури SDN дуже уразливими для збоїв і атак. Так як контролер являється головним елементом мережі, який управляє всіма видами потоків даних і самою мережею. Саме тому контролер мережі SDN має сенс резервувати, для того, щоб вразі відмови певних функцій контролера або раптової відмови самого контролера, мережа не припиняла свою працездатність.

Для таких цілей існує три види резервування [3].

Холодне резервування (cold standby) - передбачає елементи які не використовуються на постійній основі, а вмикаються тільки в момент відмови основного елементу.

Тепле резервування (warm standby) - Передбачає періодичну передачу конфігурації з основного елемента на резервний і перемикання системи на резервний компонент в разі відмови основного.

Гаряче резервування (hot standby) - передбачає копіювання конфігурацій при кожній їх зміні на резервне устаткування, і перемикання на резервний компонент у разі відмови основного.

Специфікація OpenFlow v1.5.1 говорить про те що комутатор може встановлювати зв'язок з одним контролером або з декількома контролерами. Наявність декількох контролерів підвищує надійність, оскільки комутатор може продовжувати роботу в режимі OpenFlow в разі збою одного контролера або підключення іншого контролера. Передача між контролерами ініціюються самими контролерами, що забезпечує швидке відновлення після збою, а також балансування навантаження контролера. Контролери координують управління комутатором між собою, і мета множинного контролера функціональність

призначена тільки для допомоги в синхронізації передач обслуговування контролерів, які виконуються контролерами. Мультифункціональність контролера враховує тільки відмова контролера і балансування навантаження, але не віртуалізація, яка може виконуватися поза протоколом комутатора OpenFlow. Коли запускається операція OpenFlow, комутатор повинен підключатися до всіх контролерів, з якими він налаштований, і підтримувати зв'язок з усіма ними одночасно. Багато контролерів можуть відправляти команди для перемикавання на комутатор, відповідь або повідомлення про помилки, пов'язані з цими командами, повинні бути тільки відправлені на з'єднання контролера, пов'язане з цією командою [1].

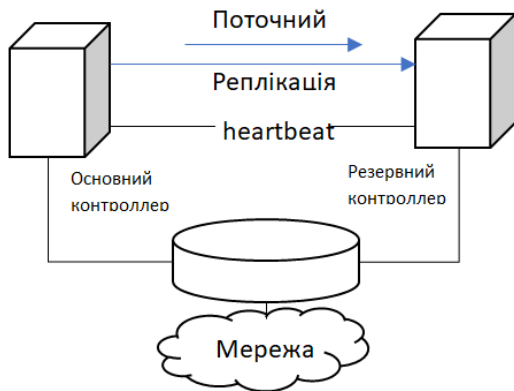


Рис. 1. З використанням роздільного сховища даних.

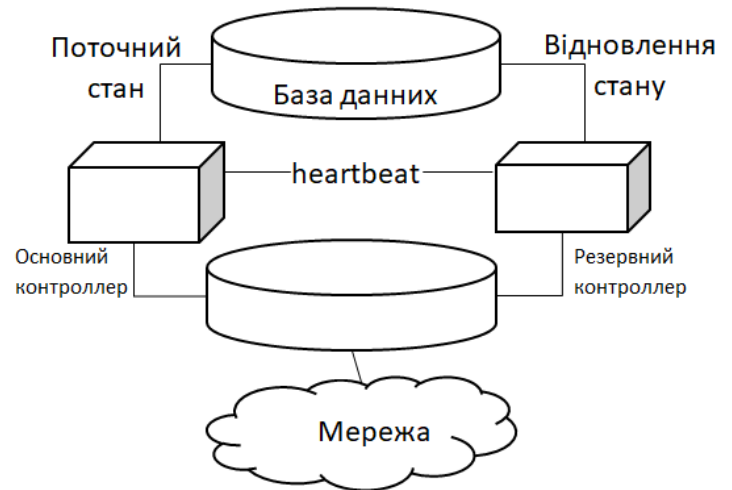


Рис. 2. З використанням механізму реплікації даних.

Останнім часом були внесені пропозиції щодо фізичного розподілу рівня управління SDN або з ієрархічною організацією, квартирною організацією. Ці підходи дозволяють уникнути використання єдиної точки відмови і дозволяють збільшити розподіл навантаження між декількома контролерами. Однак ці розподілені площини управління SDN були розроблені для центрів обробки даних, де екземпляри контролерів обмінюються величезним обсягом інформації для забезпечення точної узгодженості в масштабі всієї мережі [2].

Також існує пропозиція DISCO, відкрита площина управління розподіленої SDN для багатодоменної мережі SDN. Він заснований для організації на рівні домену, де кожен контролер DISCO відповідає за домен SDN, і забезпечує унікальний легкий і добре керований канал управління, який використовується агентами. Агенти можуть бути динамічно підключені до різних контролерів домену. домени об'єднують інформацію в масштабі всієї мережі, отже, надають наскрізні мережеві послуги [2].

Загальна архітектура DISCO (Distributed Multi-domain SDN **C**ontrollers) - це розподілена мультидоменна площина управління SDN, яка забезпечує доставку наскрізних мережевих послуг. Контролер DISCO відповідає за мережевий домен і взаємодіє з сусідніми доменами для обміну агрегованою інформацією в масштабі всієї мережі для цілей управління наскрізним потоком [2].

Контролер складається з декількох модулів (Рис. 3.), керованих компонентом Core. Він дозволяє запускати, зупиняти, оновлювати модулі і забезпечує їх

комунікаційною шиною. В архітектурі використовуються класичні готові модулі, які надають контролери SDN, такі як драйвер OpenFlow для реалізації протоколу OpenFlow, диспетчер комутаторів і диспетчер вузлів для відстеження різних мережевих елементів, а також виявлення каналів, що реалізує протокол LLDP [2].

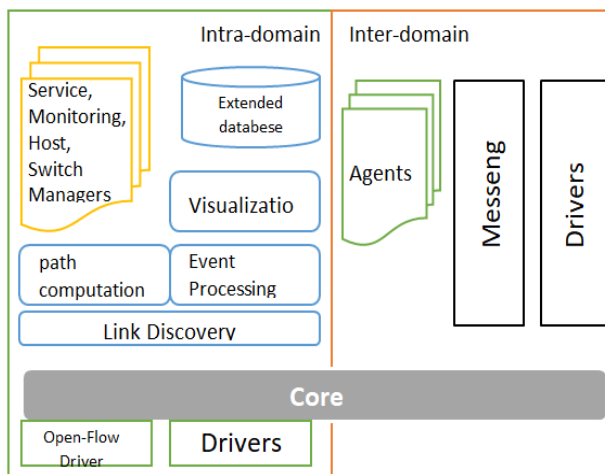


Рис. 3. Архітектура контролера DISCO.

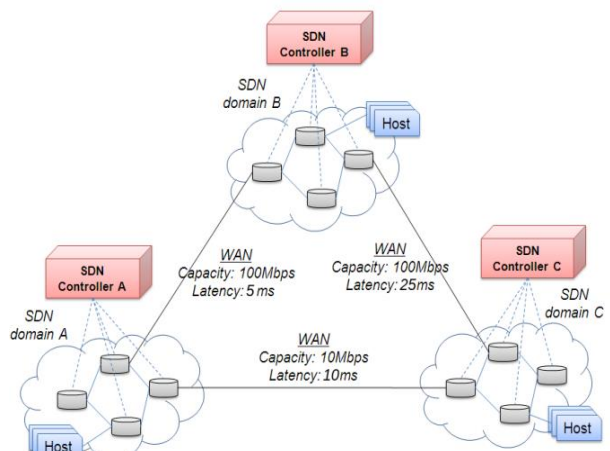


Рис. 4. Багато домена топологія SDN.

Архітектура DISCO дозволяє мережі самостійно адаптуватися відповідно до умов мережі. Для того, щоб зменшити навантаження на мережу, агенти DISCO визначають альтернативні маршрути для зменшення навантаження на канали з низькою пропускнуою здатністю. Одним із варіантів також є зменшення частоти керуючої інформації для звільнення каналу, якщо альтернативних маршрутів не існує. Кожен агент передає службову інформацію кожні 2с, для каналів з низькою пропускнуою здатністю цей інтервал може збільшуватись до 10с [2].

В ситуації коли відбувається збій каналу між контролерами, архітектура здатна відновити данні про хости та міждоменну топологію мережі до 9с.

Визначити слабкий канал та адаптувати мережу під дану ситуацію від 9с до 33с [2].

Система також має здатність перенести віртуальну машину із одного домену на інший. Якщо віртуальна машина переміщається з одного домену на інший, то віртуальна машина яка була встановлена на домені на який перемістилась нова віртуальна машина, повідомляє про те що вона не керує цим доменом, а нова віртуальна машина навпаки відправляє повідомлення всім іншим елементам мережі про те, що тепер вона керує цим пристроєм. Таке перемикання займає в середньому 117мс. З невеликими втратами пакетів [2].

Такий підхід забезпечує рівномірне розподілення трафіку, а також міграцію віртуальних машин з більш пріоритетним трафіком на домени з більшою пропускнуою здатністю каналу, але не забезпечує резервацію контролерів та збереження інформації яка доступна на цих контролерах.

Наша пропозиція закладається в тому щоб виділити на кожному контролері певну кількість пам'яті, куди періодично буде записуватись конфігурація із сусідніх контролерів через спільну базу даних (див. Рис. 5.). В такому випадку система зможе зберегти свої поточні показники передачі інформації. При виході із ладу одного із контролерів, комутатор зможе здійснити перемикання на сусідній контролер та без великих перебоїв продовжити свою роботу. Таким чином ми

зможемо застосувати тепле резервування контролерів SDN. І в разі нестачі інформації при виході із ладу одного із контролерів, сусідні контролери зможуть підтягнути її з бази даних.

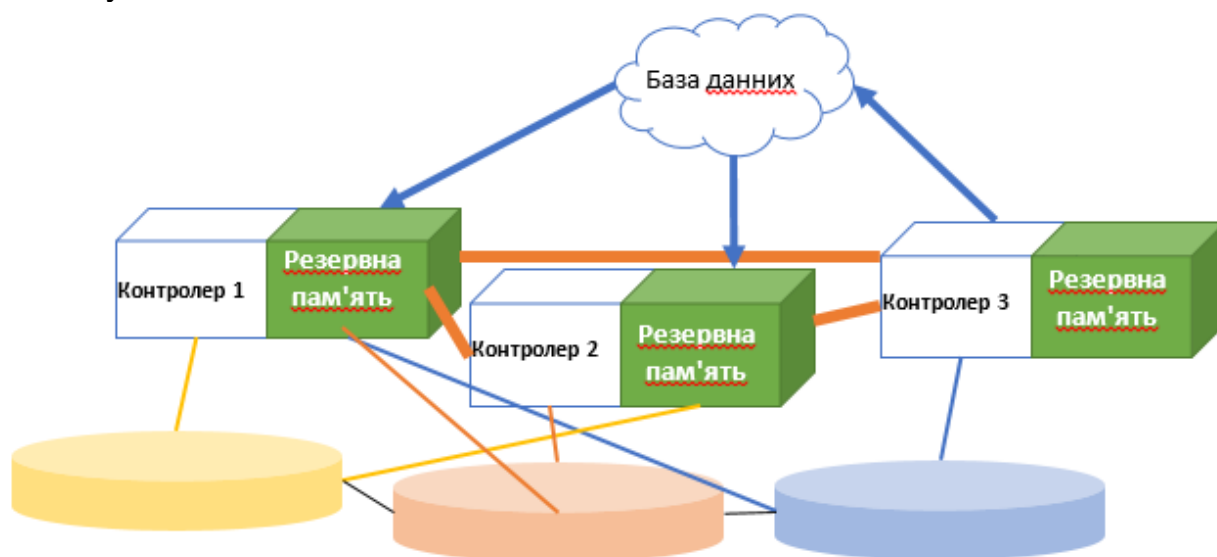


Рис. 5. Архітектура мережі SDN з резервуванням конфігурації контролерів за допомогою спільної бази даних.

В роботі пропонується використовувати резервування для підвищення функціональності систем за допомогою спільної бази даних. Таким чином аналіз проведений в цій статті дозволяє рекомендувати використовувати пропозиції закладені в системі DISCO для керування мережею та зменшення навантаження на елементи мережі. Для резервування мережі використовувати спільну базу даних яка б надавала можливість контролерам використовувати данні з сусідніх контролерів. Резервування дозволить підвищити показники надійності функціонування та зробить систему більш гнучкою у використанні.

Література

1. "OpenFlow Specification 1.5.1" - Open Networking Foundation, March 15, 2015
2. Kevin Phemius, Mathieu Bouet and J' er ' emie Leguay Thales Communications & Security «DISCO: Distributed Multi-domain SDN Controllers» 4 avenue des Louvresses, 92230 Gennevilliers, France
3. Скулиш, М. А., Романов О. І., Глоба Л. С. Принцип резервування ресурсів у віртуалізованому середовищі для контролю показників обслуговування / Скулиш М. А., Романов О. І., Глоба Л. С. // Вісник Інженерної академії України. – 2018. – С. 197-202. <https://ela.kpi.ua/handle/123456789/36912>
4. Романов, ММ Нестеренко, НО Фесьоха. Аналіз сучасних технологій віртуалізації для побудови інформаційно-телекомунікаційних систем/ОІ Романов, ММ Нестеренко, НО Фесьоха//Збірник наукових праць ВІТІ].-2019.-Вип. 1.-С. 82-90.-: http://nbuv.gov.ua/UJRN/Znpviti_2019_1_13.

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ SDN ПРИ ПОБУДОВІ КАМПУСНОЇ МЕРЕЖІ LI-FI

Романов О. І., Шаповалов Р. С.

Інститут телекомунікаційних систем КІП ім. Ігоря Сікорського, Україна

E-mail: a_i_romanov@ukr.net, shapovalovroman7@gmail.com

USING OF SDN TECHNOLOGY IN THE CONSTRUCTION OF THE LIFI NETWORK OF CAMPUS

The principles of construction and features of the functioning of campus wireless access networks based on Li-Fi technology that meet the requirements of the IEEE 802.15.7 standard are considered. Possible directions of practical implementation of VLC systems are analyzed. To solve the problems of network management, it is proposed to use the SDN technology.

Подальший розвиток систем безпроводового доступу найближчим часом може зіткнутися з низкою проблем. Це обмеженість частотного спектра, низька енергоефективність радіосистем, обмеження на використання радіозв'язку (наприклад, в літаках, лікарнях та ін.), недостатня безпека (радіохвилі можуть проникати крізь стіни і надавати шкідливий вплив на біологічні та технічні об'єкти).

Одним з можливих напрямків вирішення цих проблем є застосування Li-Fi технології. В такій системі замість звичних радіочастот для передачі даних використовується світло. Причому можуть бути використані світлові хвилі як області інфрачервоного (ІЧ) діапазону випромінювання, так і хвилі спектру видимого світла. Сьогодні вважається більш перспективним побудова телекомунікаційних систем з використанням спектра частот видимого світла (VLC).

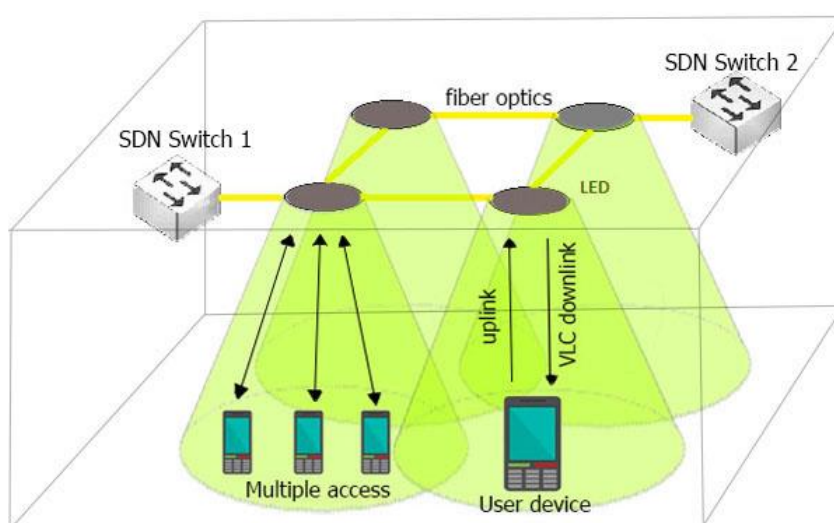


Рис.1. Варіант кампусної мережі LI-FI.

На рисунку 1 представлено варіант побудови кампусної мережі Li-Fi, який розглядається в ряді сучасних статей [1, 2].

Мережа Li-Fi включає кілька точок доступу для підключення до висхідної, низхідної та зворотної ліній зв'язку. Крім того, система забезпечує функції передачі та прийому інформації, підтримки мобільності користувачів і можливість гнучкого доступу до ресурсів. Для цього в мережі є наступні елементи:

1. LED лампа, яка забезпечує безпроводову передачу інформації з використанням VLC.
2. Fiber optics - лінії, які з'єднують LED лампи, комутатори та інше.
3. SDN Switch, який забезпечує встановлення шляху передачі між точками доступу в різних кімнатах.
4. User device - пристрій користувача, який підключається до точки доступу та отримує доступ до передачі даних.
5. Uplink. Висхідна лінія зв'язку для передачі даних з телефона на мережу, підтвердженнь передачі, інформації про стан каналу (CSI).
6. VLC downlink. Низхідна лінія зв'язку для завантаження даних з мережі.
7. Reverse transferring - взаємодія між точками доступу та мережевим комутатором.

Користувач підключається до певної точки Li-Fi доступу так само, як і до точки доступу WiFi. Завдяки цьому він отримує доступ до мережі. Він може завантажувати файл по низхідній лінії зв'язку, або навпаки вивантажувати інформацію по висхідній лінії. Користувач в процесі переміщення змінює точку доступу. Переключення відбувається автоматично без розриву зв'язку. Взаємозв'язок елементів мережі забезпечується оптоволоконною лінією, чи по мережі живлення. Якщо потрібно встановити зв'язок між точками доступу, які знаходяться в різних кімнатах, використовуються комутатори SDN Switch.

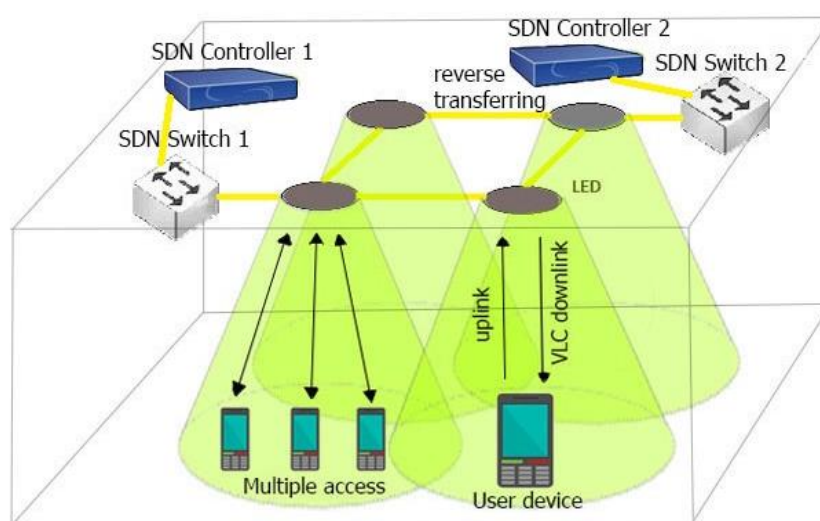


Рис.2. Кампусна мережа Li-Fi з використанням контролерів SDN.

Процес функціонування мережі достатньо складний. Користувачі рухаються в приміщенні. При цьому змінюються кути передавання і

приймання сигналів, відстань між елементами системи, зони обслуговування LED. При цьому необхідно забезпечувати вимоги до рівня освітлення в кожній точці приміщення. Тому для вирішення цих питань пропонується використовувати контролер SDN.

Сьогодні консорціум ONF проводить розробку ряду платформ з відкритим вихідним кодом. Тому в якості централізованого пристрою управління мережею LiFi можливо рекомендувати контролер SDN. За основу можна взяти контролер, який розроблений для управління ЦОД. Тоді структура мережі LI-FI буде мати вигляд, який представлений на рис.2.

Тоді принцип обміну даними в системі LiFi буде наступний (рис.3). Данні з Internet чи Server поступають на Lamp Driver, який управляє LED lamp [3]. Lamp Driver забезпечує модуляцію сигналів даних і управляє мерехтінням LED. Світловод передає цифрові дані 0 та 1. Дані містяться в світлі і приймаються світлочутливим пристроєм, який називається фотодетектором. Далі перетворення світлових сигналів на цифрові сигнали. Тракт передачі сигналів представлений на рис.3.

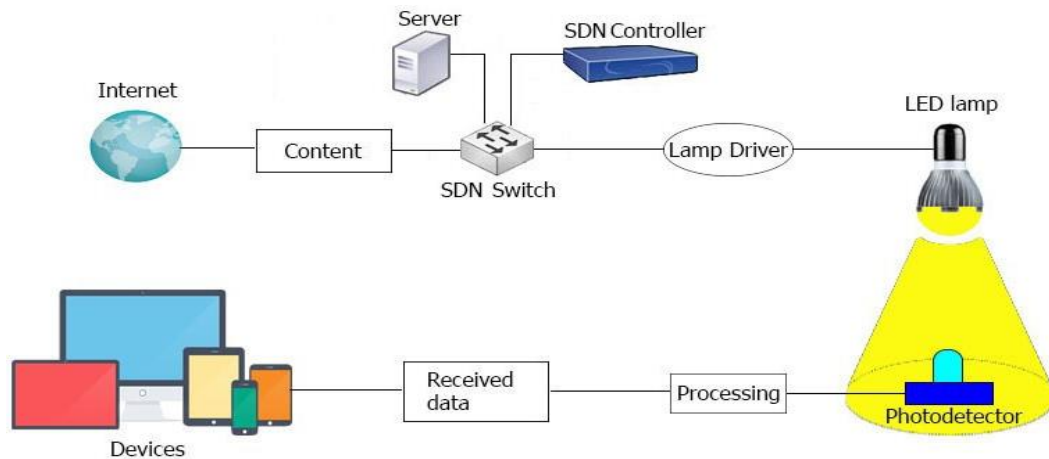


Рис. 3. Тракт передачі сигналів в Li-Fi.

Таким чином, використання принципів SDN в системах Li-Fi дозволить автоматизувати процес налаштування системи, централізовано управляти параметрами системи, забезпечити вимоги до якості обслуговування та пропускної здатності.

Література

1. Mohammad Dehghani Soltani, Ardimas Purwita, Harald Haas. Impact of Device Orientation on Error Performance of LiFi Systems. // January 2019, DOI: 10.1109/ACCESS.2019.2907463.
2. Iman Tavakkolnia, Lethy K. Jagadamma, Rui Bian, Pavlos P. Manousiadis, Stefan Videv1, Graham A. Turnbull , Ifor D. W. Samuel, Harald Haas. Organic photovoltaics for simultaneous energy harvesting and high-speed MIMO optical wireless communications // 2021, <https://strathprints.strath.ac.uk/75042/>
3. Oleksandr Romanov, Tho Dong and Mikola Nesterenko. The Possibilities for Deployment Eco-Friendly Indoor Wireless Networks Based on LiFi Technology/ 8th International Conference on Applied Innovations in IT, (ICAII), March 2020. <http://dx.doi.org/10.25673/32747>,

ПОБУДОВА SDN МЕРЕЖІ ШИРОКОСМУГОВОГО ДОСТУПУ НА БАЗІ ПЛАТФОРМИ RESIDENTIAL CORD

¹Кочура М.Ю., ²Романов М.О.

¹*Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна*

²*Факультет аеронавігації, електроніки та телекомунікації НАУ*

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

CONSTRUCTION SDN BROADBAND ACCESS PLATFORM BASED RESIDENTIAL CORD

The principle of building an SDN broadband access network based on the Residential CORD platform is considered. A list of the main elements, their purpose and functions is considered.

Розглянуто принцип побудови SDN мережі широкосмугового доступу на базі платформи Residential CORD. Розглянуто перелік основних елементів, їх призначення та функції.

Сьогодні ведуться активні наукові розробки по створенню різних видів телекомунікаційних мереж на базі концепції SDN. Одним з важливих напрямків досліджень є створення провідних мереж широкосмугового доступу на базі платформи Residential CORD (R-CORD) [1,2].

R-CORD надає послуги, які використовують технології проводового широкосмугового доступу, такі як GPON, G.Fast, 10GPON і DOCSIS. Перший етап розробки включає створення дезагрегованого і віртуалізованого пристрою OLT для GPON, яке отримало назву vOLT. R-CORD також передбачає створення віртуального абонентського шлюзу (vSG) і віртуального маршрутизатора vRouter, який надає базову мережеву послугу. При цьому, vSG реалізується у вигляді контейнера, який прив'язаний до кожного користувача. А vRouter є керуючим додатком ONOS [3,4].

Найбільш важливим функціональним елементом системи є vRouter. Тому більш детально розглянемо особливості його функціонування. Основне призначення vRouter є:

- бути шлюзом між інфраструктурою CORD і мережею більш високого рівня (наприклад, базової мережею);
- забезпечити доступ абонентам до мережі Інтернет і надання послуг в рамках CORD. Це остання служба в ланцюжку, яку проходить призначений для користувача трафік перед виходом із системи CORD.
- фізично це інтерфейс між CORD і мережею провайдера. Служба vRouter надає Інтернет як послугу для інших служб. vRouter реалізований як додаток для управління мережею, що працює на ONOS.

Вимоги до служби vRouter:

- рішення задач одноадресної маршрутизації;

- забезпечення підтримки протоколів динамічної маршрутизації (наприклад, OSPF і BGP);

- пересилання багатоадресної сигналізації (наприклад, PIM-SSM).

Дизайн служби vRouter розділений на дві частини, які відносно незалежні один від одного:

- площину управління;
- площина даних.

У кожного vRouter є кілька пристроїв dataplane, якими він управляє. Ці пристрої виглядають так, як якщо б вони були одним шлюзом, що підтримує набір протоколів маршрутизації.

У площині управління основна функціональність vRouter стосується обміну протоколами маршрутизації з зовнішніми маршрутизаторами. Щоб уникнути реалізації протоколів маршрутизації в додатку ONOS, використовується існуючий стек маршрутизації з відкритим вихідним кодом під назвою Quagga. Quagga підтримує широкий спектр протоколів маршрутизації, що дозволяє vRouter підтримувати ці протоколи без необхідності їх повторної реалізації.

Quagga забезпечує взаємодію з маршрутизаторами більш високого рівня, які використовують протоколи OSPF і iBGP.

Quagga визначає інтерфейс, званий FIB Push Interface (FPI). Він дозволяє передавати маршрути зовнішнім об'єктам [5,6]. Інтерфейс FPI забезпечує передачу маршрутів від Quagga до ONOS. Додаток ONOS vRouter діє як менеджер площині пересилання (FPM) і може приймати і декодувати маршрути від Quagga. Після цього додаток vRouter може використовувати ці маршрути для відповідного програмування площині даних. Архітектура рівня управління vRouter представлена на рис.1.

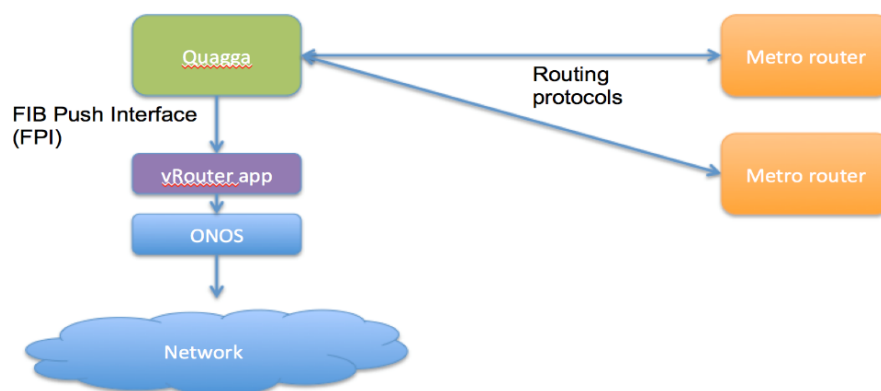


Рис. 1. Архітектура рівня управління vRouter.

Щоб Quagga могла взаємодіяти з маршрутизаторами вищого рангу, трафік управління маршрутизацією повинен проходити між сервером Quagga і зовнішнім маршрутизатором (рис.2). Перед обміном будь-якими маршрутами перше завдання додатку vRouter - це запрограмувати площину

даних так, щоб дозволити проходження цього трафіку. Сервер Quagga підключається до порту каналу даних vRouter, і пакети маршрутизації перехоплюються з відповідних портів.

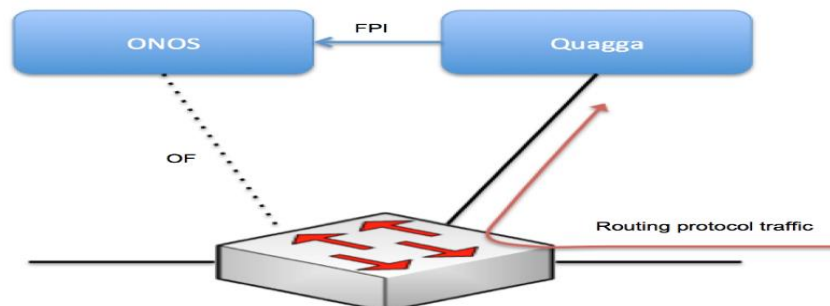


Рис. 2. Обробка трафіку управління маршрутизацією.

Елементи площини даних, з якими спілкується vRouter, - це комутатори базової мережі, які мають канали до вищих маршрутизаторів. vRouter програмує маршрути і записує їх в комутатори.

Реалізація програми vRouter в ONOS буде використовувати існуючий код з інших додатків маршрутизації ONOS.

Таким чином, Enterprise CORD є універсальною платформою, що дозволяє забезпечити підключення підприємств до широкосмугових мереж на базі програмних продуктів з відкритим вихідним кодом. Це дозволяє, по-перше, створити універсальне середовище моніторингу, що збирає показники продуктивності фізичних пристроїв і елементів програмного забезпечення в CORD. і по-друге, розробити аналітичні додатки, які динамічно адаптують CORD з урахуванням робочого навантаження і аномальних подій.

І що важливо, це вже інтелектуальна система, яка дозволяє підключатися до різноманітних віртуальних сервісів, розташованих в хмарі. Клієнти можуть швидко отримувати необхідні послуги та створювати свої мережі. При цьому налаштування, масштабування та створення нових послуг не потребує великих зусиль.

Література

1. Residential CORD. <https://wiki.opencord.org/display/CORD/Residential+CORD>, 2021.
2. Romanov O.I., Oryschuk M.V., Hordashnyk Y.S. Computing of influence of stimulated Raman scattering in DWDM telecommunication systems//2016 International Conference Radio Electronics & Communications (UkrMiCo), 2016.
3. Романов О.І., Діденко І.В. Особливості взаємодії контролера і мережевих пристроїв в мережах SDN з використанням протоколу OPENFLOW//Матеріали одинадцятої МНТК «ІТ-2017» 2017.
4. Enterprise CORD. <https://wiki.opencord.org/display/CORD/Enterprise+CORD>, 2020.
5. Романов А.И., Фигурный С.С. Повышение эффективности функционирования и защиты информации в VPN-сетях на базе технологии MPLS// Вісник УНДЗ, 2008.
6. Романов О.І., Нестеренко М.М., Верес Л.А. Модель розрахунку пропускної спроможності ІР-мультимедійної підсистеми (IMS)// Збірник наукових праць ВІПІ, 2017.

MININET: СИМУЛЯТОР ДЛЯ СТВОРЕННЯ І ПРОЕКТУВАННЯ ПРОТОТИПІВ МЕРЕЖ SDN

Бурлака Г.Ю.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: fastmotion1111@gmail.com

MININET: A SIMULATOR FOR EMULATING AND PROTOTYPING SOFTWARE-DEFINED NETWORKS

The concept of software-defined networking (SDN) fundamentally changes the way networks operate and how they are managed. In the rapidly changing modern world, it is the data transmission networks that have been called the "thin link" that limits the growth of application performance as the number of mobile users grows, virtual environments scale, and clusters are formed for Big Data. In SDN networks, traffic switching tasks and control tasks are strictly separated. All control logic is centralized and transferred to the controller.

Останнім часом сильно змінилися концепції обробки і все частіше мережа стає обмежуючим фактором розвитку обчислювальної інфраструктури. Причина полягає в тому, що мережі є статичними, на відміну від серверів, які зобов'язані цим технології віртуалізації. Якщо необхідно, наприклад, внести одну невелику зміну на шляху від однієї віртуальної машини до іншої, то максимум, чого можна домогтися, автоматизації розгортання необхідних налаштувань на обладнанні одного модельного ряду конкретного виробника. Для вирішення цих проблем була розроблена концепція SDN (Software Defined Networks) [1].

Концепція програмно-визначених мереж (SDN) ґрунтовно змінює принципи функціонування мереж і їх управління. У швидко мінливому сучасному світі саме мережі передачі даних були названі «тонким ланкою», яке обмежує зростання продуктивності додатків по мірі зростання кількості мобільних користувачів, масштабування віртуальних середовищ, формування кластерів для Великих Даних. У SDN мережах завдання комутації трафіку і завдання управління строго розділені.

Вся логіка управління централізується і передаються контролеру. Комутатор в концепції SDN - досить примітивний пристрій, який відповідає тільки за перемикання пакетів на підставі дуже простих правил. Контролер SDN управляє всіма комутаторами в мережі і програмує кожен з них для правильної передачі трафіку [2]. Централізація логіки управління дозволяє програмувати мережу як єдине ціле і спростити операційну модель великих корпоративних мереж, які занадто статичні на даний момент і не відповідають сучасному бізнесу, з властивими йому мобільністю користувачів / пристроїв / додатків, розподілом додатків між віртуальними машинами і інтенсивним обміном даними.

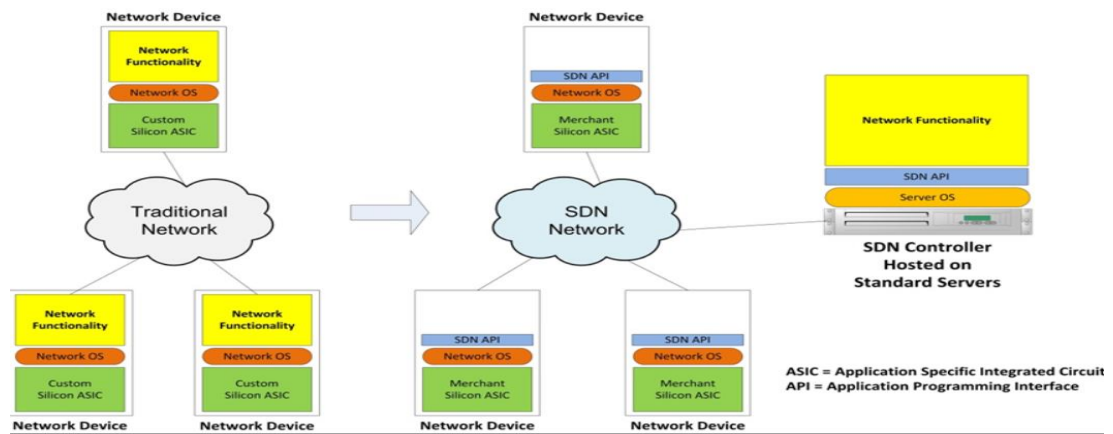


Рис. 1. Перехід від традиційної мережі до SDN.

Завдяки контролеру з розширеними API інтерфейсами, вся мережа стає подібною одному великому логічному комутатору. Протокол OpenFlow - один з найбільш універсальних протоколів комунікації контролерів і комутаторів на сьогоднішній день надає стандартний підхід до програмування таблиць комутації, в яких основним об'єктом є потік даних. Однак в той час як OpenFlow дозволяє контролеру програмувати комутатори, він не визначає, як контролера реагувати і відповідати на виклики, пов'язані з хмарами, BYOD, BYOC, віртуалізацією. Рішення будь-яких проблеми з продуктивністю мережі, та й просто її роботою, покладені на контролер і додатки, які на ньому запуснені. Саме набір таких додатків і відрізняє різні впровадження SDN, а також рішення різних виробників [3].

Для проектування і тестування мереж SDN дуже зручно використовувати симулятор Mininet (рис. 2). Він дозволяє створити мережу віртуальних хостів, комутаторів, контролерів і посилань. Хости Mininet запускають стандартне мережеве програмне забезпечення linux, а його комутатори підтримують OpenFlow для дуже гнучкою, що настраюється маршрутизації і програмно визначається мережі. Mininet підтримує дослідження, розробки, навчання, створення прототипів, тестування, налагодження і будь-які інші завдання, які можуть виграти від наявності повної експериментальної мережі на ноутбуці або іншому ПК. Mininet надає простий спосіб отримати правильну поведінку системи (і, наскільки це підтримується вашим обладнанням, продуктивність), а також поекспериментувати з топологіями.

У мережах Mininet працює реальний код. Через цей код ви розробляєте і тестуєте на Mininet, для контролера OpenFlow, модифікованого комутатора або хоста, можете перейти на реальну систему з мінімальними змінами для реального тестування, оцінки продуктивності та розгортання. Важливо, що це означає, що проект, який працює в Mininet, зазвичай може переходити безпосередньо до апаратних комутаторів для пересилання пакетів на лінійній швидкості [4].

Mininet може створювати комутатори OpenFlow в ядрі або призначеному для користувача просторі, контролери для управління комутаторами і хости для зв'язку з модельованою мережі. Mininet з'єднує комутатори та хости за

допомогою віртуальних пар Ethernet (veth). Код Mininet майже повністю написаний на Python, за винятком невеликої утиліти C .

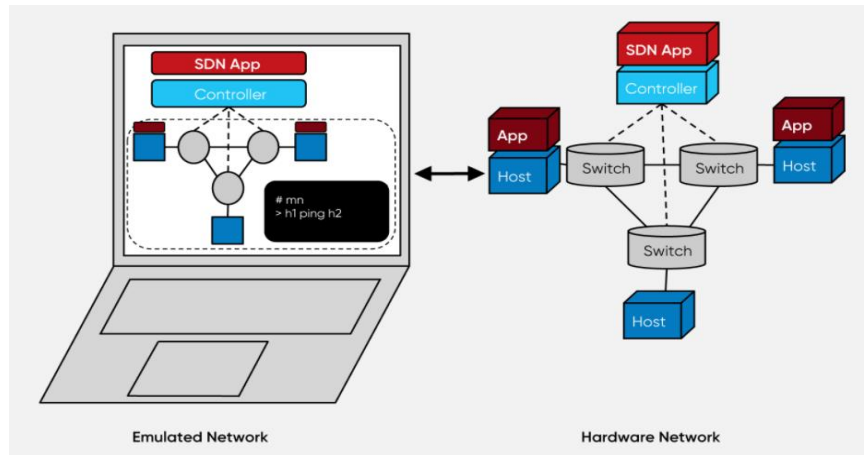


Рис. 2. Структурно - функціональна схема Mininet.

Коли дві програми, такі як клієнт і сервер *iperf*, обмінюються даними через Mininet, виміряна продуктивність повинна відповідати продуктивності двох (більш повільних) власних машин. Простіше кажучи, віртуальні хости, комутатори, посилення і контролери Mininet справжні - вони просто створюються з використанням програмного забезпечення, а не обладнання - і здебільшого їх поведінку схоже на дискретні елементи обладнання [5].

Таким чином, технологія Mininet зручна для створення прототипів і моделювання. Це альтернатива тестуванню реальних мереж, які потребують великих затрат. Створення віртуальної мережі в Mininet дозволяє швидко протестувати системи різної конфігурації

Література

1. Bruno Astuto A. Nunes, Marc Mendonca, Xuan-Nam Nguyen, Katia Obraczka, Thierry Turlétti, "A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks", Vous Consultez L'Archive Hal, 19 Jan, 2014.
2. McKeown, Nick, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, and Jonathan Turner. "OpenFlow: enabling innovation in campus networks." *ACM SIGCOMM Computer Communication Review* 38, No. 2 (2008): 69–74.
3. Mininet as Software Defined Networking Testing Platform [Електронний ресурс]: https://www.researchgate.net/publication/287216738_Mininet_as_Software_Defined_Networking_Testing_Platform.
4. Carapinha, J., Feil, P., Weissmann, P., Thorsteinsson, S., Etemoglu, Ç. Ingþórsson, Ó., Çiftçi, S., Melo, M., "Network Virtualization: Opportunities and Challenges for Operators," *Future Internet-FIS 2010*: 138–147, 2012.
5. Using Mininet for emulation and prototyping Software-Defined Networks [Електронний ресурс]: https://www.researchgate.net/publication/269292945_Using_Mininet_for_emulation_and_prototyping_Software-Defined_Networks.

ЗАСАДИ ПРОЕКТУВАННЯ ОФІСНОЇ МЕРЕЖІ НА БАЗІ ТЕХНОЛОГІЇ Li-Fi

Мікляєв Г.О.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: glibmiklaiv@gmail.com

FOUNDATIONS OF OFFICE NETWORK DESIGN BASED ON LI-FI TECHNOLOGY

The paper discusses the basics of designing an office network based on Li-Fi technology. The system transmits a signal in monochromatic light with movable terminals and immovable emitter. The project was designed using MATLAB software.

В роботі розглянуто засади проектування офісної мережі на базі технології Li-Fi. Система в роботі передає сигнал у монохромному світлі з рухомими терміналами та нерухомим випромінювачем. Спроековано за допомогою програмного забезпечення MATLAB.

Сьогодні основною технологією надання мобільного інтернету користувачам є технологія Wi-Fi. Однак вона має ряд недоліків:

1. Знаходиться на межі можливостей по пропускній здатності, про що попереджує федеральна комісія США з радіозв'язку [1];
2. Використання технології пов'язано з великими затратами на електроживлення;
3. Має обмеження на використання в лікарнях, літаках та інших місцях;
4. Використовує обмежену полосу радіочастот.

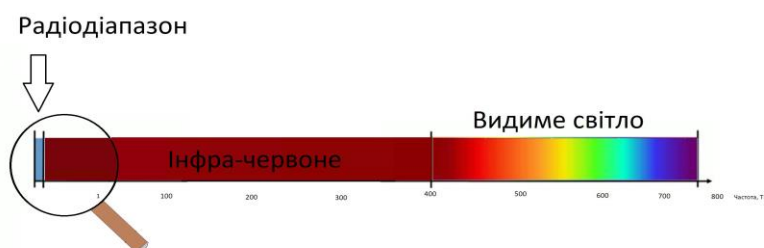


Рис. 1. Використання діапазону Li-Fi в 1000 разів більше.

Тому в роботі пропонується використовувати нову технологію в якій замість радіохвиль використовуються світлові хвилі - це технологія Li-Fi [2, 3], вона має наступні переваги:

1. Діапазон використовуваних частот збільшується в 10'000 разів [2]. А це можливості значного підвищення пропускної здатності.
2. Екологічно чиста та безпечна для здоров'я технологія [4, 5, 6].
3. Можна використовувати готову інфраструктуру освітлення на LED лампах в якості готової мережі передавання даних.

На сьогоднішній день системи поки що Li-Fi досліджуються в лабораторних умовах.

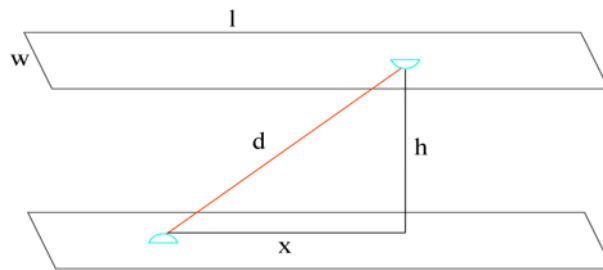


Рис. 2. Проста модель, у якій термінал і передавач нерухомі.

Для вирішення поставленої задачі спочатку автором розроблено просту модель, яка зображена на рис.2. В цій моделі передавач та приймач користувача нерухомі. Далі було розроблено ускладнену модель. Ця модель враховує рух терміналів (зображення на рис. 3).

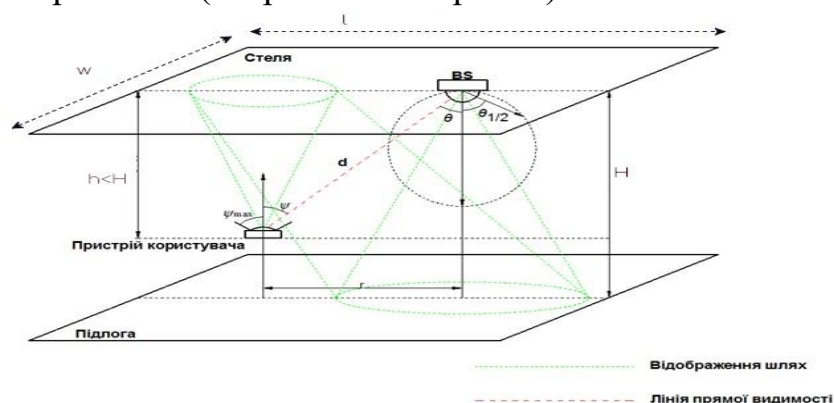


Рис. 3. Складна модель, в якій термінал рухається, і кути змінюються.

Надалі було вирішено ще одну проблему. Оскільки потрібно розраховувати потужність сигналів не в одній точці кімнати, а по всій її площині підлоги, автором написано програму з використанням програмного забезпечення MATLAB, котра зображена на рис. 4.

```

1 phi_b=7*pi./18;
2 fov=pi./3;
3 n=1.5;
4 S=0.001;
5 Psi_mx=pi./2;
6 l=6;
7 w=6;
8 h=3;
9 T=1;
10 Gfov=(n./sin(Psi_mx)).^2;
11 m=-log(2)./log(cos(phi_b));
12 g_phi=n.*n./sin(fov);
13 xmas=[0:0.1:l];
14 ymas=[0:0.1:w];
15 [x,y]=meshgrid(xmas,ymas);
16 dist=sqrt((l./2-x).^2+(w./2-y).^2+h.^2);
17 cosang=(h./dist);
18 Hlos=S.*(m+1)*cosang.^m.*T.*Gfov./(2.*pi.*dist.^2);
19 pcolor(xmas,ymas,Hlos);
20 shading interp;
21 Z=colorbar;
22 Z.Label.String = 'Потужність, Вт';

```

Рис. 4. Програма у ПЗ MATLAB.

Згодом автор вдосконалив програму з метою представлення розрахунків у вигляді графіків, зручних для аналізу результатів. Результат у вигляді графіку представлено на рисунку 5.

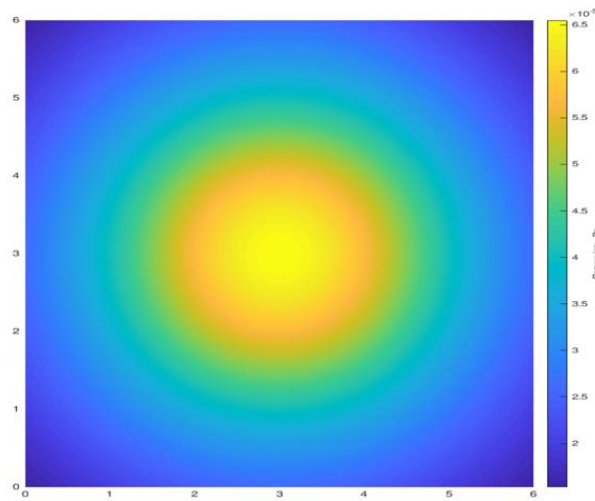


Рис. 5. Результат обрахунку, приймаюча потужність в залежності від положення в кімнаті.

Висновки.

В роботі показано, що для того, щоб в майбутньому користувачі отримували послуги з більш високими швидкостями, більшою пропускнуою здатністю, високою якістю обслуговування та з використанням екологічно чистих систем, необхідно використовувати технологію Li-Fi. Для вирішення цієї задачі автором було розроблено:

- модель офісної системи Li-Fi з рухомими об'єктами,
- програму розрахунку параметрів системи Li-Fi з використанням програмного забезпечення MATLAB,

Всі напрацювання представлено в роботі у вигляді метода розрахунку параметрів офісної системи Li-Fi з рухомими терміналами в зручній наглядній формі.

Література

1. Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021 White Paper.
2. D.Tsonev, S.Videv, and H.Haas, “Towards a 100Gb/s visible light wireless access network”, Optics Express, vol.23, no.2, pp.1627-1637, Jan. 2015.
3. FN Division, TEC “Study Paper on LiFi (Light Fidelity) & its Applications” http://tec.gov.in/pdf/Studypaper/lifi_study_paper_-_approved.pdf.
4. CELMA, Optical safety of LED lighting. URL: [http://www.lightingeurope.org/uploads/files/CELMAELC_LED_WG\(SM\)011_ELC_CEMA_position_paper_optical_safety_LED_lighting_Final_1st_Edition_July2011.pdf](http://www.lightingeurope.org/uploads/files/CELMAELC_LED_WG(SM)011_ELC_CEMA_position_paper_optical_safety_LED_lighting_Final_1st_Edition_July2011.pdf).
5. Pingree T.L., Dangers of Overexposure to ultraviolet, infrared and high-energy visible light. URL: <http://www.ishn.com/articles/94815-dangers-of-overexposure-to-ultraviolet-infrared-and-high-energy-visible-light>.
6. Hranilovic S. and Kschischang F.R., Optical Intensity-Modulated Direct Detection Channels: Signal Space and Lattice Codes, Information Theory, IEEE Transactions Volume 49 Issue 6, pp. 1385 -1399, 28-05-2003.

ОЦІНКА БЕЗПЕКИ ТА АНАЛІЗ ВРАЗЛИВОСТІ IP MULTIMEDIA SUBSYSTEM (IMS)

Полуденний О. М., Цуканов О. Ф.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: alexpoludenniy@gmail.com

IP MULTIMEDIA SUBSYSTEM (IMS) SECURITY ASSESSMENT. VULNERABILITY ANALYSIS OF IMS.

NGN introduces the concept of fix-mobile convergence (FMC). NGN provides the IP multimedia subsystem (IMS) as platform to converge the wire and wireless networks. It is open and distributed architecture that can enable easy access to services, information and resources. But the same time there is lot of risks in such approach. Potential hackers can access IMS architecture to launch some attacks on IMS network. IMS security is vital important and it is beneficial to be aware of possible vulnerabilities. This paper investigates current situation in IMS security regulations, potential threats and attacks facing to IMS deployment. We also provide vulnerability discovering and analysis method with Open Source IMS Core.

Оцінка безпеки IMS проводиться на основі двох підходів:

1. eTVRA.
2. Архітектура безпеки ITU-T. 805.

Подібності в архітектурній структурі можуть бути знайдені між IMS і ITU-T X. 805, який є рекомендаціями МСЕ-Т для наскрізних комунікацій. У цих рекомендаціях серії X. 800 загрози визначаються, як знищення інформації і ресурсів, пошкодження або зміну інформації, крадіжка або видалення даних, розкриття інформації та переривання роботи служб. Вони були запропоновані в якості основи для архітектури NGN для досягнення наскрізної безпеки в розподілених додатках (Atay and Masera, 2011). X. 805 складається з 3 архітектурних частин: розміри безпеки, рівні безпеки і площини безпеки, як показано на рис. 1.

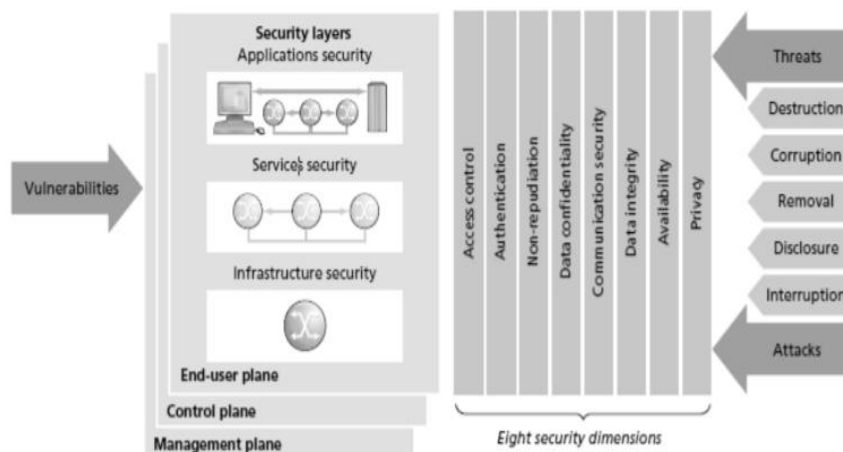


Рис. 1. ITU-T X. 805.

Рівні безпеки також складаються з 3-х рівнів: рівень інфраструктури, рівень безпеки сервісу, рівень безпеки сервісу. Площина безпеки показує дії, які відбуваються на площині безпеки мережевого управління, площині безпеки управління і площині безпеки кінцевого користувача.

Безпека вимірювання - це методи забезпечення безпеки, спрямовані на захист: контроль доступу, аутентифікацію, відмова від анулювання, конфіденційність даних, безпека потоку зв'язку, цілісність даних, доступність та конфіденційність. Кожен рівень

пов'язаний з унікальними вразливостями, погрозами та заходами щодо їх усунення.

Одним із стандартів оцінки безпеки є стандарт ISO 15408: 2009 загальні критерії оцінки безпеки інформаційних технологій, але цей стандарт є дорогим по часу і ресурсам. З цієї причини програма конвергенції телекомунікаційних послуг та протоколів для передових мереж (TISPAN) в Європейському інституті стандартів телекомунікацій (ETSI), найбільшій європейській організації по стандартизації телекомунікацій (Telco) з світовим впливом, розробила метод аналізу загроз, вразливостей і ризиків (eTVRA) для підтримки телекомунікаційних компаній у загальній оцінці критеріїв безпеки.

Оцінка уразливості в eTVRA складається з 7 етапів, показаних на рис.2. (Moralı et al., 2009). Процес починається з визначення цілей безпеки системи або системного компонента, з яких вилучаються вимоги безпеки.

Надалі складається опис активів в системі. Мета використання eTVRA полягає в тому, щоб мати можливість ідентифікувати проблеми, які існують в системі. Тому після ідентифікації активів, визначаються проблеми, загрози, які використовують ці уразливості і викликають інциденти. Вимоги безпеки і загрози розширюються у відповідності з погрозами і вразливостями. Потім проводиться аналіз і кількісна оцінка ймовірності виникнення загроз і їх впливу. Це використовується в наступному кроці для розрахунку ризику. Отже, визначені контрзаходи для обробки ризику. Цей процес застосовується ітеративно, до тих пір, поки ризик небажаних інцидентів не буде знижено до прийняттого рівня, або всякий раз, коли відбуваються зміни в навколишньому середовищі (Rosseb et al., 2006).

В ході дослідження використаємо X. 805 модульні перспективи безпеки, які показані на РИС. 3. (Anon, 2011.) для аналізу основних вразливостей IMS, який показано з допомогою eTVRA.

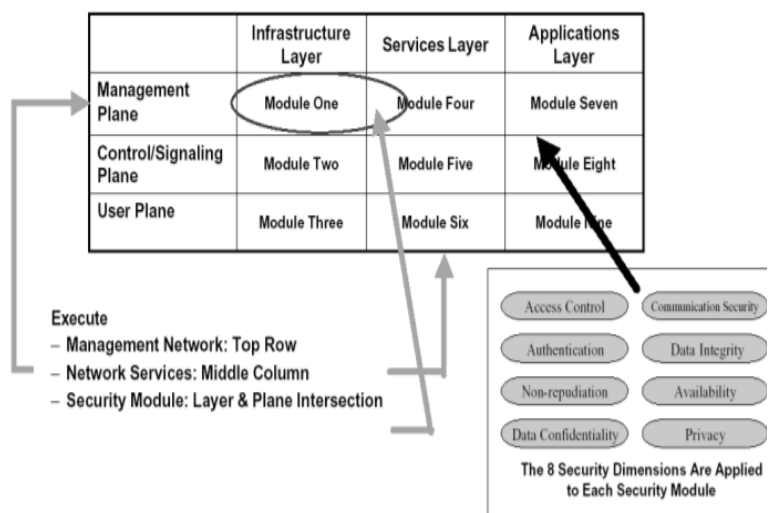


Рис. 3. Модульні перспективи безпеки з X. 805.

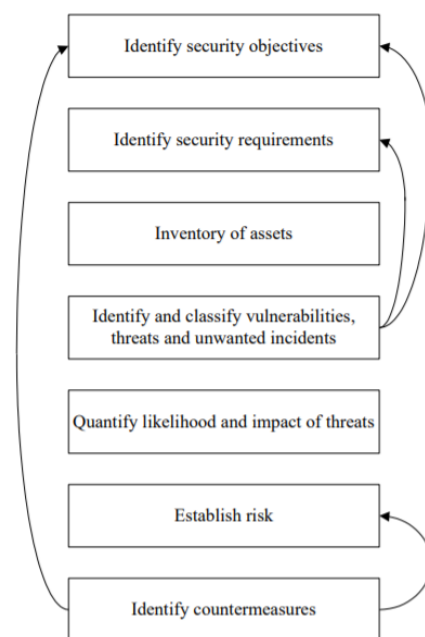


Рис. 2. Основні етапи роботи eTVRA.

Існує 9 точок зору або модулів безпеки, де необхідно ідентифікувати програмні та апаратні засоби. В кожній точці зору, в якості третього фактору в аналізі уразливості повинен бути включений людський фактор, який означає, що повинні бути оцінені всі види діяльності, а також таке рішення повинно забезпечувати не тільки аналіз вразливостей, але і кращу реалізацію та поліпшення безпеки, оскільки така модель дозволяє оновлювати безпеку при виявленні вразливостей.

Стандарти та протоколи постійно змінюються. IMS є досить новою архітектурою в

мережах і знаходиться в процесі дослідження, вона буде змінюватись, виправлятись, розвиватись, і будуть інтегруватися нові функції. Це означає, що аналіз вразливостей повинен постійно оновлюватися і контролюватися з кожною зміною в системі.

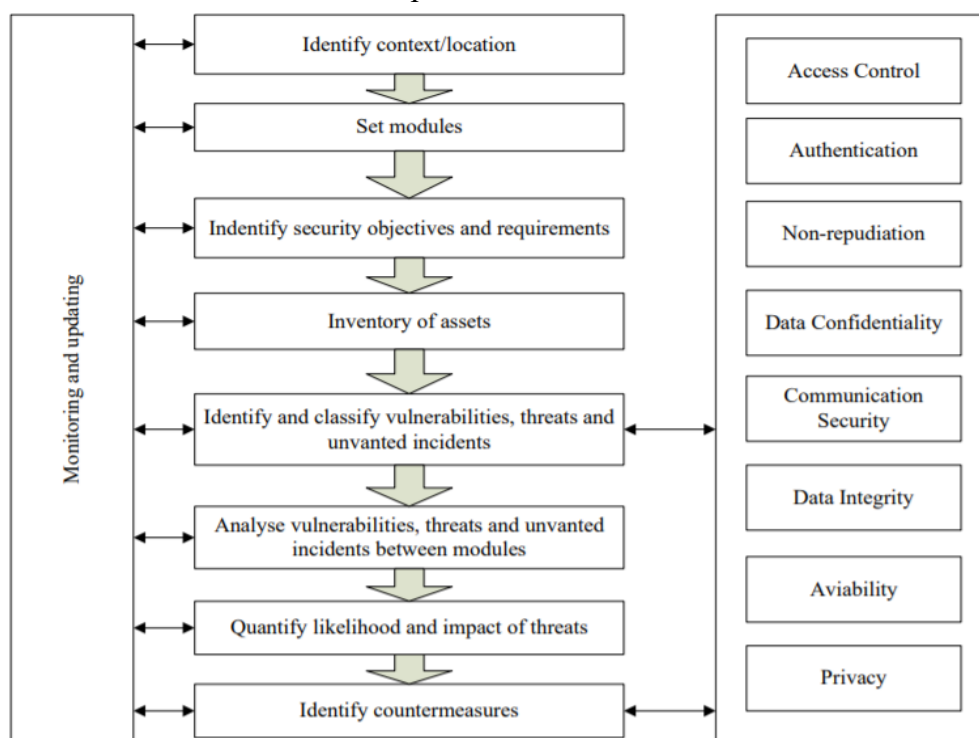


Рис.4. Розширена модель тестування вразливостей IMS.

Процес дослідження показав, що не всі аспекти безпеки можуть бути адресовані кожному модулю, але в будь-якому випадку вони повинні бути проаналізовані в контексті інфраструктури та основних елементів. Будь-який об'єкт з певною функціональною цінністю в цій архітектурі може бути проаналізований як основний елемент, який повинен бути згрупований у відповідності з його конкретним рівнем безпеки і площиною, що показано в таблиці 1. Аналіз вразливості IMS був проведений згідно з категоризацією основних елементів.

Таблиця 1. Основні елементи концепції IMS.

IMS assets by modules			
	Infrastructure Layer	Service Layer	Application Layer
Management plane	CTF, CDF, CGF, PDF	Diameter (Rf, Rx, Ro) COPS (Go)	HTTP (Ut)
Control plane	CSCF, MGCF, MRFC, BGCF, IBCF, SLF, AS, DNS, ENUM	SIP/SDP(Gm, Mw, Mg, Mi, Mj,Mk, Mr), Diameter(Ch, Dx), H248 (Mp, Mn)	SIP(ISC), Diameter(Sh, Dh)
End-user plane	IM-MGW, MRFP, HSS, UE	RTP/RTCP(Mb), User profile	Voice, IM, VIDEo, State(XCAP)

Аналіз вразливостей IMS показав, що IMS може піддаватися різним типам атак. Тестування уразливості проводилося на відкритому тестовому стенді IMS. Це ядро вихідного коду проекту є відкритою частиною платформи IMS і використовується для налаштування тест-стенду для практичного моделювання сценарію. В таблиці 2 наведено результати поточного дослідження різних вразливостей системи безпеки.

Більшість заходів безпеки виявляються стандартними механізмами, такими як IPSec і TLS або аутентифікація і авторизація. Але такі атаки, як SQL-запити, не можуть бути захищені і вимагають додаткового інструменту реалізації найбільш ефективного захисту, метод захисту повинен мати інструмент виявлення і запобігання вторгнень. Це допомогло б покращити захист від загроз пов'язаних з людським фактором.

Висновки. Отже, розглянуто реалізацію моделі eTVRA в аналізі вразливостей IMS,

яка доповнюється рекомендаціями ITU-T X. 805 безпеки. Пропонується метод для повного покриття тестування вразливостей. У роботі були показані основні загрози і майбутня кількісна оцінка вразливостей та її аналіз. Також, як перспективна технологія для захисту може бути впровадження системи виявлення та запобігання вторгнень. Дослідження показують, що найбільша вразливість пов'язана з рівнем додатків і площиною управління, що означає, що цим частинам потрібно приділяти додаткову увагу для захисту.

Таблиця 1. Результати поточного дослідження різних вразливостей системи безпеки.

IMS vulnerability list				
Vulnerability	Weakness	Security dimension	Asset module	Impact
Message spoofing	IMS has absence of IPsec protection between user equipment and P-CSCF	Authentication	Service layer Control plane	Fraud of trust
SIP SQL injection	SIP authentication controllability is insecure	Availability	Service layer User plane	Denial of service
Media theft	Not enough control on media streams	Non-repudiation	Infrastructure layer Management plane	Theft of services
SIP flooding	Unable effectively prevent REGISTER and INVITE message flooding	Availability	Infrastructure layer Control plane	Loss of QoS for users
RTP data sniffing	No default confidentiality from data stream	Confidentiality	Application layer User plane	Theft of information
CANCEL attack	Possibility to fake SIP CANCEL request	Integrity	Service layer Control plane	Session disruption
RTP injection	RTP protocol missing media integrity protection mechanisms	Integrity	Service layer User plane	Session disruption
Man in the Middle P-CSCF attack	Authentication using SIP must be improved	Authentication	Service Layer Control plane	Impersonation of a server
Dictionary attack	Inadequate identity protection and AKA chipper algorithm use	Authentication	Application layer Control plane	Identity theft
BYE attack	Possibility to fake SIP BYE request/ not enough confidentiality protection	Integrity	Service layer Control plane	Disruption of session
DNS Cache Poisoning	Not enough connection integrity protection	Integrity	Infrastructure plane Control plane	Loss of service
Network topology disclosure	Not protected SIP messages	Confidentiality	Infrastructure layer Control plane	Leak of network topology
HTTP Parse Attack	Improperly data ContentLength regulation	Availability	Infrastructure layer Control plane	Loss of services
User equipment configuration tampering	Probability lack of user education in security questions	Availability	Infrastructure layer Control plane	Denial of services

Література

1. IP Multimedia Subsystem - IP Multimedia Subsystem [Електронний ресурс] – Режим доступу до ресурсу: https://ru.qwe.wiki/wiki/IP_Multimedia_Subsystem#Charging.
2. IP Multimedia Subsystem (IMS) Handbook / Ahson S.A., Ilyas M., 2009. – 562 с.
3. Developing SIP and IP Multimedia Subsystem (IMS) Applications.. – 690 с.
4. F. Galán. Design and Implementation of an IP Multimedia Subsystem (IMS) Emulator Using Virtualization Techniques : дис. канд. техн. наук / F. Galán.. – 12 с.

МЕТОД РОЗРАХУНКУ НАДІЙНОСТІ РІВНЯ УПРАВЛІННЯ АРХІТЕКТУРИ IMS ПРИ КОВЗНОМУ РЕЗЕРВУВАННІ

Верес Л.А.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: veresleonid@gmail.com

METHOD FOR CALCULATING THE RELIABILITY OF THE IMS ARCHITECTURE CONTROL LEVEL WITH MOVING RESERVATION

Due to the fact that in Ukraine not so long ago, mobile operators launched 4g networks and used them only to increase the data transfer speed, and to introduce new services such as VoLTE and VoWiFi, an architecture is needed that can ensure the correct operation of voice services using packet data transmission. But since mobile operators will still use 2G and 3G networks to service voice traffic for a long time, therefore, one of the necessary conditions for the normal functioning of mobile operators' networks is the introduction of the IP Multimedia Subsystem (IMS) as the main element of the control level. One of the main requirements for the IMS system is the requirement for its reliability.

В Україні всі оператори мобільного зв'язку проголосили про запуск мереж 4g. Основна відмінність цих мереж – більш висока швидкість передачі даних. Однак мережі 4g повинні надавати нові послуги, наприклад такі як VoLTE і VoWiFi через пакетну мережу передачі даних. А для цього необхідна нова архітектура рівня управління IP Multimedia Subsystem (IMS), яка представлена на рис.1. Одною з основних вимог до системи IMS є висока надійність функціонування [1].

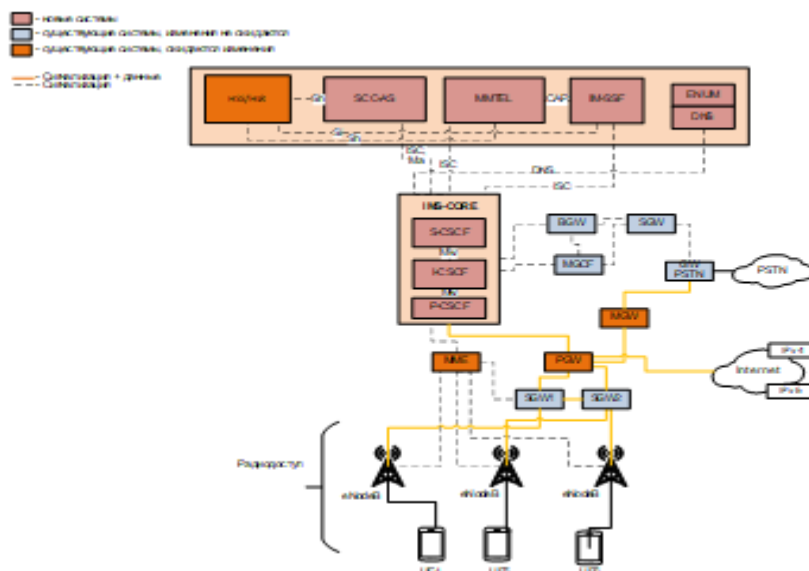


Рис.1. Архітектура мережі 4G з використанням IMS.

Розглянемо кілька причин необхідності надійності. Перша причина є зростання складності мобільних мереж, апаратури їх обслуговування, жорсткості умови експлуатації та відповідальності завдань, які на них покладаються [2]. Недостатня надійність мережі мобільного оператора призводить до збільшення частки експлуатаційних витрат у порівнянні з

загальними витратами. При цьому вартість експлуатації IMS може у багато разів перевершити вартість їх розробки і впровадження. Крім того, відмови IMS призводять різного роду наслідків: втрат інформації, простоїв пристроїв і систем. Третьою причиною підвищення ролі надійності в сучасних умовах є економічний фактор. Втрата сервісу у клієнта веде до втрати прибутку оператора. Одним з методів забезпечення високої надійності є метод ковзного резервування.

Ковзне резервування використовується для резервування кількох однакових елементів системи одним або декількома однаковими резервними елементами. Це говорить про те що буде кілька головних елементів без яких система не буде працювати і кілька надлишкових. Така система називається система типу "m з n" [3, 4,] представлена на рис.2. Наприклад, візьмемо систему з кількох елементів. Вони повинні бути з однаковою надійністю і повинен бути ще один або кілька елементів які в разі падіння одного з головних елементів візьмуть на себе це навантаження і цей елемент повинен бути підключений до всіх елементів що б система працювала правильно. Цю модель резервування можна застосувати і для архітектури IMS на рівні управління. Рівень управління має три функціональні елементи I-CSCF, S-CSCF, P-CSCF [5]. Так як ці елементи виконують різну роль на рівні управління то вони мають різний функціонал, але фізично вони можуть мати однакову продуктивність і надійність. Таким чином ми можемо застосувати цей вид резервування для архітектури IMS.

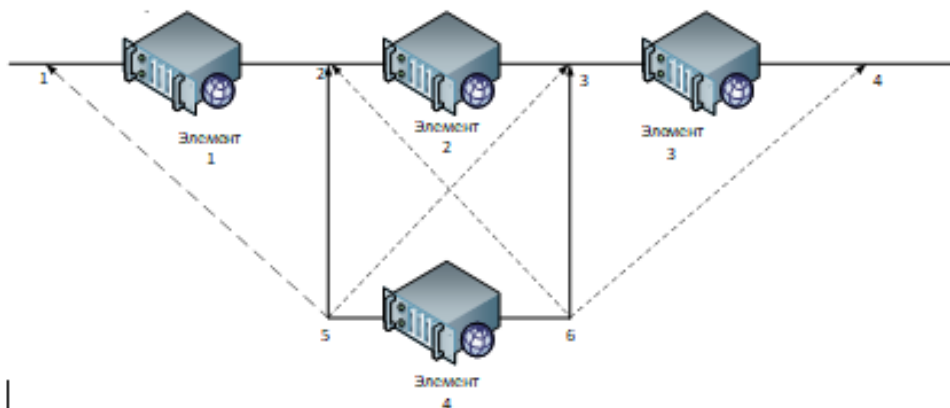


Рис.2. Модель ковзного резервування 3 з 4.

Розрахунок надійності системи "m з n" може проводитися комбінаторним методом, в основі якого лежить формула біноміального розподілу. Біноміальному розподілу підпорядковується дискретна випадкова величина k - кількість працюючих елементів, n - максимальна кількість всіх елементів, без яких система працювати не буде, p - надійність одного елемента. При цьому ймовірність події визначається:

$$P_k = C_n^k p^k (1 - p)^{n-k}$$

де C_n^k - біноміальний коефіцієнт, "числом елементів 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 $k = 0, 1, \dots, (n-1)$:

$$Q = \sum_{k=0}^{m-1} P_k = \sum_{k=0}^{m-1} C_n^k p^k (1-p)^{n-k}$$

Аналогічним чином можна знайти надійність всієї системи як суму для $k = m, m+1, \dots, n$:

$$P = \sum_{k=m}^n P_k = \sum_{k=m}^n C_n^k p^k (1-p)^{n-k}$$

Наведемо приклад розрахунку ковзного резервування на рівні управління архітектури IMS рис.2, коли в ядрі системи є 4 елементи з яких три мають працювати обов'язково. Тоді підставимо в формулу: $m=3$; $n=4$;

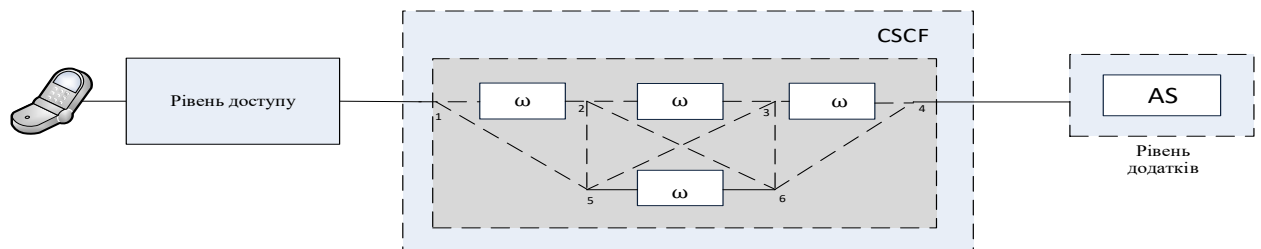


Рис.2. Модель ковзного резервування рівня управління IMS з елементами однакової надійності.

$$W_{\text{CSCF SKOL REZ}} = \sum_{k=3}^4 P_k = \sum_{k=m}^n C_n^k p^k (1-p)^{n-k} = \sum_{k=3}^4 C_4^3 p^3 (1-p)^{4-3}$$

Таким чином, використання моделі та наведених формул дозволяє розрахувати показники надійності системи IMS для методу ковзного резервування.

Література

1. O.I. Romanov, M.M. Nesterenko, L.A. Veres. IMS: Model and calculation method of telecommunication network's capacity // UkrMiCo. 2017, DOI: 10.1109/UkrMiCo.2017.8095412.
2. Mariia Skulysh, Romanov Oleksandr. The structure of a mobile provider network with network functions virtualization. //TCSET, IEEE, 2018 P-1032 - 1034 DOI: 10.1109/TCSET.2018.8336370.
3. Глазунов Л.П. и др. Основы теории надежности автоматических систем управления: Учеб. пособие для вузов. – Л.: Энергоатомиздат, ленингр. отд-ние, 1984. – 208 с.: ил.
4. Abhayawardhana V.S., Babbage R. A traffic model for the IP Multimedia Subsystem (IMS) // 2007, IEEE Magazine, – C.783 – 787.
5. Romanov, O., Nesterenko, M., Veres, L., Kamarali, R., Saychenko, I. Methods for calculating the performance indicators of ip multimedia subsystem (IMS) // Lecture Notes in Networks and Systems, 2021, 152, с. 229-256 .

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

УДК 621.396

**ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ
ІНФОРМАЦІЇ В СУПУТНИКОВІЙ СИСТЕМІ ІНТЕРНЕТУ
РЕЧЕЙ НА БАЗІ ПРОТОКОЛУ LoRaWAN**

¹Новіцька А.О., ¹Капштик С.В., ²Наритник Т.М.

¹*Національний центр управління та випробувань космічних засобів, Україна*

²*Інститут телекомунікаційних систем КІІ ім. Ігоря Сікорського, Україна*
E-mail: s.kapshtyk@spacecenter.gov.ua; director@mitris.com

**FEATURES OF INFORMATION SECURITY IN THE SATELLITE
INTERNET OF THINGS SYSTEM BASED ON THE LoRaWAN PROTOCOL**

Features of the Internet of Things satellite systems design using the LoRaWAN protocol are considered. The prospects of transferring the key element of the system - the LoRaWAN gateway to the space segment are shown. The proposals for the distribution of LoRaWAN information security tools have been developed, taking into account the peculiarities of the low-Earth-orbit satellite system. The advantages of inter-satellite-links introducing to the architecture of the Internet of Things satellite system constellation based on the LoRaWAN protocol for the implementation of information protection mechanisms in the LoRaWAN satellite system are shown.

Важливою складовою частиною діяльності щодо впровадження систем та послуг Інтернету речей [1-3] є формування телекомунікаційної інфраструктури, необхідної для передачі інформації від сенсорів – пристроїв Інтернету речей, призначених для перетворення фізичних параметрів контрольованих процесів в електричні сигнали і формування інформаційних посилок, та до актуаторів – пристроїв Інтернету речей, що забезпечують формування керуючих впливів на підставі отриманих інформаційних посилок – команд керування.

Завдяки своїм перевагам технологія мережі передачі повідомлень Інтернету речей LoRaWAN [4] активно застосовується в супутникових низькоорбітальних системах Інтернету речей, що в переважній більшості створюються із використанням космічних апаратів класу куб-сат (масою 1-10 кг) [5]. Зокрема, компанія SWARM розробляє супутникову систему, що буде побудована із використанням куб-сатів, і буде використовувати протокол LoRaWAN [6]. Але недоліком такого підходу є використання супутникового сегменту в якості радіоподовжувача, тобто пристрою, який приймає та перевипромінює радіосигнали, які випромінюються передавальними пристроями в межах зони радіобачення космічного апарату.

Підвищити ефективність супутникової системи, яка функціонує на базі протоколу LoRaWAN, можливо шляхом перенесення до космічного сегменту системи пристроїв зі складу інфраструктури системи LoRaWAN, які здійснюють об'єднання в єдиному потоці інформації від окремих сенсорів.

На рис.1 наведена структурна схема супутникової мережі, що побудована із використанням протоколу LoRaWAN. На відміну від запропонованих раніше рішень, до складу корисного навантаження космічних апаратів введено шлюз LoRaWAN. Космічний апарат приймає інформацію від усіх пристроїв Інтернету речей, які знаходяться в межах зони радіобачення космічного апарату, формує єдиний інформаційний потік, який передає до наземної станції спряження провайдера послуг Інтернету речей. Управління ресурсом

супутникової системи здійснює центр управління мережею LoRaWAN, який виконує функції оператора мережі, і який має окрему станцію спряження мережі. Зважаючи на особливість спрямування інформаційних потоків в мережі LoRaWAN можливо розглядати варіант використання спільної станції спряження, яка обслуговує центр управління послугами Інтернету речей, тобто провайдера послуг Інтернету речей, та центр управління мережею, тобто оператора мережі.

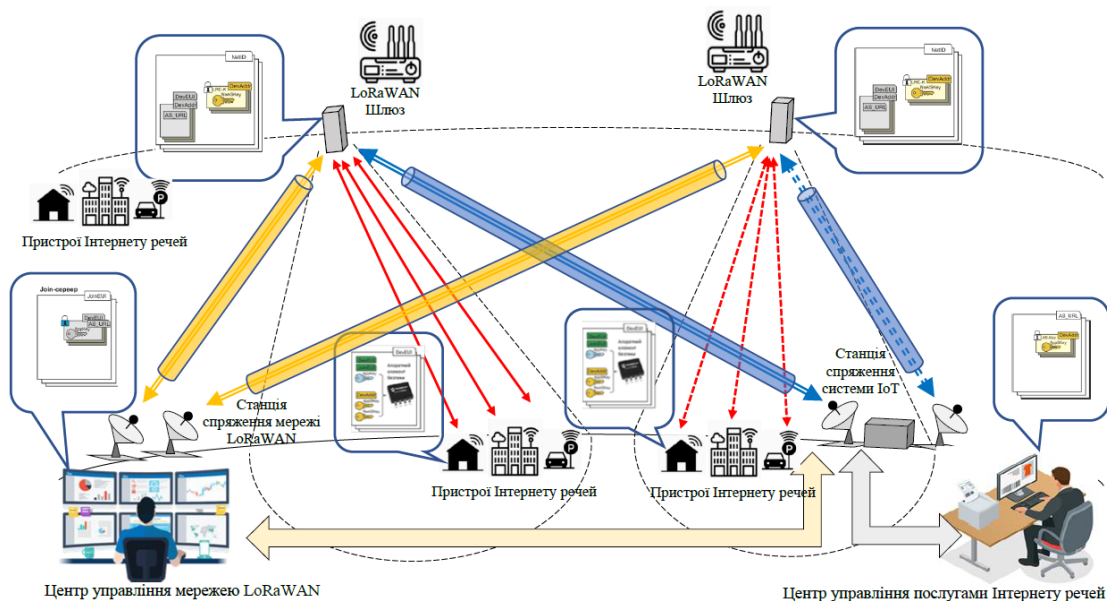


Рис. 1. Супутникова система Інтернету речей на базі протоколу LoRaWAN.

Протокол LoRaWAN передбачає використання вбудованих ефективних методів захисту інформації, які побудовані на базі алгоритму блочного шифрування AES (Advanced Encryption Standard) [7]. На мал.1 показано розподіл елементів захисту інформації по складових частинах супутникової системи. Зокрема, в кінцевому пристрої Інтернету речей (сенсори та актуатори) зберігаються ключі, що застосовуються для шифрування інформації на рівні додатків AppSKey та на рівні мережі NwkSKey. В шлюзі, який розташований у складі корисного навантаження космічного апарату, зберігається ключі доступу до мережі NwkSKey, в центрі управління мережею LoRaWAN розташований Join-сервер. Ключі рівня додатків AppSKey зберігаються в сервері додатків, який розташований в центрі управління послугами Інтернету речей.

Особливістю архітектури супутникової системи, наведеної на мал.1, є відсутність з'єднань між космічними апаратами. В наслідок цього, пристрої Інтернету речей контролюють наявність зв'язку із космічним апаратом шляхом контролю за надходженням повідомлень по лінії «до низу» у вікнах приймання повідомлень від шлюзу. В разі відсутності підтвердження від шлюзу кінцевий пристрій переходить в режим очікування і ініціює процедуру запиту доступу до мережі чергового космічного апарату, який заходить до зони радіобачення пристрою Інтернету речей. Кінцевий пристрій LoRa ініціює JOIN процедуру. Спочатку до супутника передається запит для приєднання JOIN_REQUEST, який складається з ідентифікатора додатку (AppEUI), ідентифікатора пристрою (DevEUI) і випадкового числа (DevNonce), що використовується при розрахунку ключів NwkSKey і AppSKey. Після підтвердження запиту, шлюз і кінцевий пристрій генерують однакові ключі за допомогою DevNonce. В результаті кінцевий пристрій передає повідомлення JOIN_ACCEPT. Така архітектура супутникової системи представляє систему як сукупність мікро радіомереж LoRaWAN, що сформовані окремими космічними апаратами. Керування інформаційним обміном та безпекою таких мікро радіомереж LoRaWAN здійснюється із застосуванням технології тунелювання IP-трафіку між станціями спряження та шлюзами LoRaWAN окремо для кожного космічного апарату.

Введення до складу космічного сегменту супутникової системи ліній зв'язку між космічними апаратами дозволяє підвищити гнучкість системи, подовжити строк використання розрахованих ключів, скоротити частоту виконання процедури запиту на входження до мережі LoRaWAN кінцевих пристроїв Інтернету речей (рис.2).

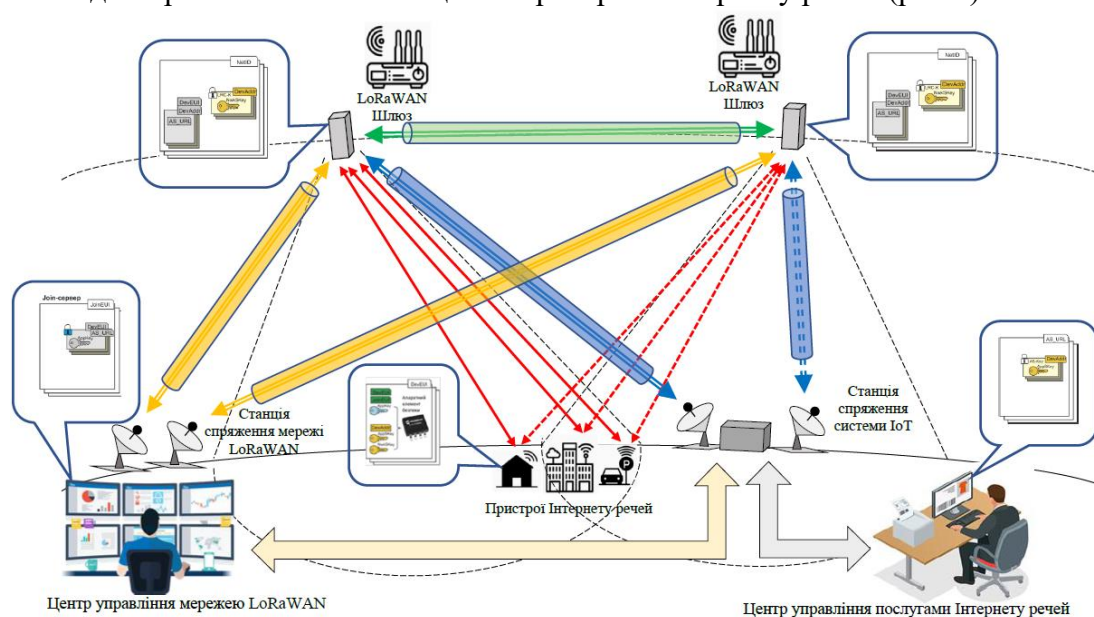


Рис.2. Модифікована супутникова система Інтернету речей на базі протоколу LoRaWAN.

По лінії зв'язку між супутниками може передаватись масив інформації, який містить вихідні дані, що використовувались при реалізації процедури доступу кінцевих пристроїв до мережі LoRaWAN: ідентифікатор додатку (AppEUI), ідентифікатор пристрою (DevEUI), випадкове число (DevNonce). Космічний апарат, який забезпечує передачу інформації на пристрої Інтернету речей, передає до сусіднього космічного апарату, який рухається за ним, масив інформації про усі пристрої Інтернету речей, які знаходяться в межах його зони обслуговування, і які приймають участь і інформаційному обміні в мережі LoRaWAN (тобто за винятком непрацюючих пристроїв). На підставі отриманого масиву даних космічний апарат, що входить в зону радіобачення пристрою Інтернету речей, має можливість розрахувати дублікат мережевого ключа, що виключає необхідність використання процедури запиту доступу до мережі.

Ініціатива передачі управління від космічного апарату, що виходить із зони радіобачення, до космічного апарату, який входить до зони радіобачення кінцевого пристрою Інтернету речей, належить космічному апарату. Космічний апарат контролює радіоінтерфейс до кінцевих пристроїв. В разі виявлення факту отримання сигналу від кінцевого пристрою, інформаційна посилка до якого пройшла перевірку на цілісність, космічний апарат повідомляє про це попередній космічний апарат. Попередній космічний апарат надсилає кінцевому пристрою Інтернету речей інформацію про передачу управління до наступного космічного апарату. Кінцевий пристрій Інтернету речей передає тестове повідомлення до обох космічних апаратів, оскільки ще знаходиться на перетині зон обслуговування обох космічних апаратів, що рухаються один за одним. В разі отримання підтвердження від космічних апаратів про цілісність прийнятих тестових повідомлень кінцевий пристрій та шлюз космічного апарату приймають рішення про актуальність мережевого ключа та продовжують інформаційний обмін. Про вдале завершення процедури передачі тестового повідомлення та про підтвердження актуальності мережевого ключа шлюз повідомляє оператора мережі та провайдера послуг.

З метою підвищення інформаційної безпеки системи та мережі LoRaWAN, супутникова система може запроваджувати процедуру примусового виконання процедури запиту доступу до мережі для кінцевих пристроїв Інтернету речей. Період такої процедури

може становити відрізок часу, кратний періоду орбіти системи, оскільки із врахуванням обертання Землі на наступному витку орбіти космічні апарати починають обслуговувати іншу ділянку – смугу обслуговування на поверхні Землі. Таким чином до зони обслуговування космічних апаратів потрапляють інші кінцеві пристрої Інтернету речей, а до зони радіобачення кінцевих пристроїв Інтернету речей в свою чергу заходять інші космічні апарати (зі складу сусідньої орбітальної площини орбітального угруповання).

Підвищити ефективність супутникової системи, яка функціонує на базі протоколу LoRaWAN, можливо шляхом використання запропонованої схеми розподілу засобів інформаційної безпеки в супутниковій системі Інтернету речей та перенесення до космічного сегменту системи пристроїв зі складу інфраструктури системи LoRaWAN, які здійснюють об'єднання в єдиному потоці інформації від окремих сенсорів.

Введення до складу космічного сегменту супутникової системи ліній зв'язку між космічними апаратами і періодичність примусового застосування процедури запиту доступу до мережі дозволяє покращити гнучкість системи, подовжити строк використання розрахованих ключів, скоротити частоту виконання процедури запиту на входження до мережі LoRaWAN кінцевих пристроїв Інтернету речей.

В матеріалах доповіді, визначено умови застосування процедур розрахунку ключів додатків та доступу до мережі. Визначено місце реалізації процедур та методів захисту інформації зі складу протоколу LoRaWAN в супутниковій системі. Запропоновано два варіанти розподілу засобів захисту інформації для архітектури орбітального угруповання без та із лініями зв'язку між космічними апаратами.

Література

1. The computing load balancing through the orbital computer network of the internet of things (2020) / Ilchenko, M., Narytnik, T., Prisyazhny, V., Kapshtyk, S., Matvienko, S. / Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika), 79 (4), pp. 343-352. / Електронний ресурс. Режим доступу: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85085244112&doi=10.1615%2fTelecomRadEng.v79.i4.70&partnerID=40&md5=73f400a98bc0fa4ae5c25074171c5593> / DOI: 10.1615/TelecomRadEng.v79.i4.70.
2. The solution of the problem of the delay determination in the information transmission and processing in the LEO satellite internet of things system (2019) / Ilchenko, M., Narytnik, T., Prisyazhny, V., Kapshtyk, S., Matvienko, S. / 2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 - Proceedings, стаття № 9061350, pp. 419-425. / Електронний ресурс. Режим доступу: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85083638366&doi=10.1109%2fPICST47496.2019.9061350&partnerID=40&md5=7768787b80c0fd34e7417001cecc231b> / DOI: 10.1109/PICST47496.2019.9061350.
3. Ільченко М.Ю., Наритник Т.М., Присяжний В.І., Капштик С.В., Матвієнко С.А. Низькоорбітальна супутникова система Інтернету речей на базі розподіленого супутника. Космічна наука і технологія. 2020. 26. №4 (125). С.57-85. <https://doi.org/10.154307/knit> 2020.04.057.
4. Інтернет вещей: LoRa устройства от Mikrotik / Електронний ресурс. Режим доступу: <https://lanmarket.ua/stats/internet-veshchey-lora-ustroystva-ot-mikrotik/>
5. Semtech and Swarm Deliver Satellite Communications With LoRa® / Електронний ресурс. Режим доступу: <https://www.semtech.com/company/press/semtech-and-swarm-deliver-satellite-communications-with-lora>.
6. Our Technology. See how Swarm works and what makes us unique / Електронний ресурс. Режим доступу: <https://swarm.space/our-technology/>
7. Обзор технологии LoRa / Електронний ресурс. Режим доступу: <https://itechinfo.ru/content/%D0%BE%D0%B1%D0%B7%D0%BE%D1%80-%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B8-lora>.

ПРОБЛЕМИ КІБЕРБЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ

Правило В. В., Хижняк С. П.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: v.v.pravylo@ukr.net, khizhnyak56843@gmail.com

PROBLEMS OF CYBERSECURITY OF THE INTERNET OF SPEECHES

In this paper, we look at several cybersecurity issues, as well as the importance of preserving information from cyber-attacks.

Як і будь-яка інша технологія, що розвивається, Інтернет речей (IoT) також має безліч переваг та ризиків [1]. Прихильники технологій та виробники пристроїв IoT просувають Інтернет речей як засіб зробити наше щоденне життя кращим та простішим завдяки мільярдам «розумних» пристроїв IoT (наприклад, смарт-телевізори, розумні холодильники, розумні кондиціонери, розумні духовки, розумні камери, розумні кросівки, розумні дверні дзвінки, розумні системи поліцейського спостереження та дорожнього руху, інтелектуальне відстеження здоров'я та ефективності, тощо).

Є деякі проблеми, пов'язані з використанням пристроїв Інтернету речей. Загрози кібербезпеки можуть привести до пошкодження або крадіжки даних з мінімальними зусиллями з боку злочинців. Пристрої Інтернету речей нові і люди можуть скористатися недоліками кібербезпеки зі злим умислом.

Ми живемо в епоху Інтернету речей, і, хоча цифрове з'єднання - це дуже добре, воно створює безліч дрібних точок, де кіберзлочинці можуть проникнути в дані [2]. Безпека Інтернету речей спрямована на вирішення цих проблем і забезпечення безпечного використання Інтернету речей.

Багато з нас покладаються на Інтернет речей в деяких досить важливих справах в суспільстві, навіть якщо ми цього не усвідомлюємо. Комунальні підприємства, такі як енергетика і водопостачання, часто покладаються на пристрої Інтернету речей для управління ними. Датчики Інтернету речей для бізнесу допомагають забезпечити дотримання нормативних вимог і прискорити процес оплати. Коли безпека Інтернету речей знаходиться під загрозою на цьому рівні, стає ще простіше зрозуміти, чому так важливо зберігати дані в безпеці.

Якщо ви щось чуєте про технології, ви повинні знати про Штучний інтелект (ШІ) та автоматизацію. Вони вже допомагають експертам у багатьох галузях сортувати величезні обсяги даних та приймати важливі рішення. Зрештою, автоматизація та ШІ можуть бути використані в інтересах

адміністраторів Інтернету речей і співробітників служби безпеки мережі. Подібні інструменти дозволять цим сторонам виявляти потенційно проблемний трафік і шаблони даних. ШІ може навіть використовуватися для забезпечення дотримання правил, пов'язаних з даними. Але є проблема: коли люди використовують автономні системи, щоб робити вибір, який впливає на безліч реальних людей, стає дійсно очевидним, що одне незручне нелюдське рішення може завдати великої шкоди.

Отже, якщо хтось хоче найближчим часом створити додаток на основі Інтернету речей, він повинен розглянути такі проблеми безпеки, як ці. Для вирішення проблем безпеки, які створюють штучний інтелект і автоматизація необхідний: захист Інтернету речей від атак та захист призначених для користувача даних від крадіжок.

Безпека інтернету речей залишиться головним пріоритетом. Згідно з прогнозами GSMA, до 2025 року кількість підключень до IoT подвоїться і досягне майже 25 млрд в усьому світі, а в міру збільшення популярності IoT зростає ризик кібератак. Кібербезпека IoT викликає занепокоєння у 95% респондентів опитування, проведеного аналітиками IoT Analytics, причому майже 40% «дуже стурбовані» можливими вразливостями інтернету речей. 88% вказали, що підтримують впровадження правил забезпечення безпеки IoT і прийняття галузевих стандартів для управління передовими методами кібербезпеки. Передбачається, що ринок безпеки IoT виросте до \$ 36,6 млрд до 2025 року [3].

Пристрої Інтернету речей стають все більш популярними і коли ми довіряємо технологічним компаніям виробляти ці пристрої, ми повинні піти на певний ризик. Технологічні компанії не завжди проявляють належну обачність, коли справа доходить до роботи з пристроями Інтернету речей і зниження ризиків безпеки.

Багато пристроїв Інтернету речей не оновлюються [4]. Коли наші ранні комп'ютерні системи зіткнулися з тією ж проблемою, її (в деякій мірі) було виправлено за допомогою автоматичних оновлень програмного забезпечення. Але якщо справа доходить до пристроїв Інтернету речей, довговічність не завжди є пріоритетом для виробників. Немає простого способу оновлювати пристрої IoT на ходу. Виробники просто створюють щось, щоб привернути увагу своєї аудиторії, а потім працюють над наступним гаджетом, що відповідає цим вимогам. IoT-пристрої потребують належного тестування, перш ніж вони будуть випущені для широкої публіки. Поточні недостатні зусилля для цього не захищають споживачів або обладнання.

Також повинні бути чіткі стандарти безпеки, щоб забезпечувати нашу безпеку кожен день – в школі, на роботі, в Інтернеті, в транспортних засобах та стоячи перед холодильником. Стандарти безпеки, які регулюють пристрої

IoT, неясні. У кращому випадку вони неоднозначні. Більшість пристроїв Інтернету речей складається з безлічі компонентів, вироблених в усьому світі. Це тому, що частини, з яких складаються ці пристрої, дуже спеціалізовані – їх можуть робити тільки деякі сутності. Це створює проблему: коли всі частини створюються окремо, всі вони покладаються на свої власні набори стандартів безпеки. Різні стандарти безпеки роблять пристрої Інтернету речей уразливими. Коли справа доходить до захисту конфіденційності користувачів, це велика проблема.

В налаштуваннях IoT ризикованими є не тільки самі атаки, але і прогнозування і запобігання цих атак, які представляють собою найбільшу проблему. Кібератаки Інтернету речей надзвичайно непередбачувані, більшість хакерів використовують нові сучасні методи, щоб зламати систему безпеки і якомога довше уникнути виявлення. Пристрої Інтернету речей повинні мати можливість миттєво обробляти дані, що ускладнює реалізацію процесів безпеки. Ці процеси безпеки сповільнюють здатність пристрою IoT виконувати функції.

Моніторинг за допомогою ШІ може допомогти в прогнозуванні та запобігання атак в майбутньому. Експертам необхідно виявляти уразливості і усувати їх у міру їх появи.

Сучасні хмарні сервіси вже використовують аналіз загроз для прогнозування проблем безпеки. Ми поступово наближаємося до деяких рішень безпеки для Інтернету речей, але для цього потрібен час.

Ще одним складним питанням, яке потрібно вирішити, є той факт, що певні невеликі атаки IoT насправді можуть уникнути виявлення. Це робить їх особливо небезпечними. Мікропроникнення IoT легко проскакують через багато елементарних мереж безпеки, які ми використовуємо для захисту пристроїв IoT. Кіберзлочинці можуть повільно збирати інформацію, замість того, щоб одночасно передавати у власність величезну кількість записів.

Немає сумнівів що нам потрібно приділяти більше уваги кібербезпеці Інтернету речей, щоб зробити пристрої Інтернету речей більш безпечними у використанні і зберігати інформацію від атак, бо інформація у наш час безцінна.

Література

1. <https://www.rapyder.com/blogs/top-10-iot-security-solutions-for-common-iot-security-issues/>
2. <https://techcrunch.com/2015/10/24/why-iot-security-is-so-critical/>
3. <https://cutt.ly/Yxfi7xW>
4. <https://option3ventures.com/iot-security-challenges/>

ОГЛЯД ТА АНАЛІЗ ІСНУЮЧИХ АЛГОРИТМІВ РАДІОПЕЛЕНГАЦІЇ ДЖЕРЕЛ ВИПРОМІНЮВАННЯ ДЛЯ РАДІОТЕХНІЧНИХ СИСТЕМ

Авдєєнко Г.Л., Денисенко Н.І.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: djangoo2006@ukr.net, natalka.denysenko@gmail.com

OVERVIEW AND ANALYSIS OF EXISTING DIRECTION-FINDING ALGORITHMS OF RADIO SOURCES FOR RADIO SYSTEMS

Modern technological progress has complicated the radio environment, which stimulates the development of radio monitoring tools based on direction-finding methods. In order to select the optimal algorithms for radio sources direction-finding for further radio systems improvement, existing direction-finding algorithms were considered.

В даний час спостерігається стабільно зростаюче ускладнення радіоелектронної обстановки. В першу чергу це пов'язано з технічним прогресом засобів радіозв'язку. Цей прогрес, в свою чергу, стимулює розвиток засобів радіомоніторингу на основі методів пеленгації [1].

Перелік завдань, що вирішуються за допомогою засобів радіомоніторингу, включає панорамний спектральний аналіз; виявлення та аналіз радіовипромінювань для ідентифікації джерел сигналів і перешкод; визначення місця розташування джерел радіовипромінювань; моніторинг радіоканалів [2].

Завдання радіопеленгації ускладнюється наявністю великої кількості радіозасобів, які працюють в одній смузі частот, при цьому джерела радіовипромінювання можуть бути рознесені на малу відстань по азимуту. Традиційні методи пеленгації, виявляється, не в змозі розрізнити близько розташовані джерела випромінювання сигналів за пеленгом. У складній електромагнітній обстановці надають перевагу використанню методів кутового надрозширення, оскільки вони забезпечують високу точність оцінки кута приходу одного сигналу і можливість визначення пеленгів декількох близько розташованих сигналів на одній частоті [3].

Фізично в основі методів пеленгації джерел випадкових сигналів з надрозширенням лежить той же ефект, що і в адаптивній фазованій антенній решітці (ФАР) – когерентна компенсація (придушення) сигналів джерел, що заважають, при чому в якості заважаючих для кожного з джерел виступають всі інші, які не збігаються з ним у кутовому напрямку. Тому цілком звичним виявляється і спільність апарату і математичних методів, що використовуються в адаптивних ФАР і нелінійних методах з кутовим надрозширенням. Що ж стосується терміну «надрозширення», то він просто відображає більш високу роздільну здатність (по кутовим координатам) в порівнянні з релеєвською межею Δ_R типу:

$$\Delta_R = \frac{1}{N \cdot d}, \quad (1)$$

де N – число елементів антенної решітки; d – нормований по

відношенню до довжини хвилі крок (міжелементна відстань) в антенній решітці.

Алгоритмів пеленгації з надрозширенням, включаючи їх варіанти і різного роду модифікацій, дуже багато. Обмежимося перерахуванням і короткою характеристикою основних груп алгоритмів, дотримуючись класифікації [4], яка є однією з найбільш вдалих з відомих до теперішнього часу і групує алгоритми пеленгації із надрозширенням наступним чином:

- алгоритми лінійного передбачення;
- алгоритми типу Кейпон;
- проекційні алгоритми;
- алгоритми, засновані на узгодженні (підборі) параметричних моделей сигналів.

Алгоритми першої групи історично з'явилися в застосуванні до аналізу часових рядів, тобто до оцінки звичайного спектру, і можливість їх використання для оцінки просторового спектра, строго кажучи, обмежується лінійними еквідистантними решітками з рівномірним амплітудним розподілом, хоча практично застосування в нерегулярних лінійних решітках також виявляється можливим.

Алгоритм Кейпона застосовується до антенних решіток будь-якої конфігурації, в тому числі до нерегулярних і двовимірних, і дає досить низький рівень бічних пелюсток, але вимагає щодо відносно більшої кількості навчальних вибірок - принаймні, вдвічі більше в порівнянні з числом елементів решітки.

У групі проекційних алгоритмів (алгоритмів підпросторів) в першу чергу необхідно виділити алгоритм MUSIC (Multiple Signal Classification). Цей алгоритм так само як і алгоритм Кейпона, застосовується до антенних решіток будь-якої конфігурації, але потенційно перевершує алгоритм Кейпона по роздільній здатності, чим і пояснюється підвищений інтерес до нього з боку багатьох дослідників.

Остання група алгоритмів з числа перерахованих передбачає задання моделі сигналів з повним набором параметрів (напрямки, амплітуди, фази), з наступним підбором таких значень параметрів, які найкращим чином узгоджуються з результатами вимірювань. Алгоритми цієї групи відрізняються великою різноманітністю варіантів і підходів і одночасно - великим обсягом і значною складністю обчислень [4].

Метод Кейпона був запропонований в 1969 році для розрізнення спектральних компонент дискретного спектра. Використовуючи аналогію частотного і просторового спектрів, метод був запропонований також для оцінювання кутів приходу сигналів за допомогою антенних решіток [5].

Алгоритм роботи методу Кейпона складається з двох етапів. На першому етапі відбувається обчислення оцінки кореляційної матриці вхідних сигналів R . Другий етап полягає у формуванні опорного напрямку, для чого задається вектор-гіпотеза V і обчислюється цільова функція. Після чого вибирається новий опорний напрямок і повторюється процес обчислення функції. Графічним представленням цільової функції є пеленгаційний рельєф простору.

Пеленгаційний рельєф як функція кута пеленга β для методу Кейпона

формується за формулою [6]:

$$Q_c(\beta) = \frac{1}{V(\beta)^H R^{-1} V(\beta)}, \quad (2)$$

де R^{-1} – обернена кореляційна матриця сигналів з виходів елементів антенної решітки; $V(\beta)$ – вектор-гіпотеза або опорний (керуючий) вектор антенної решітки.

Відповідно до формули (2) графічне відображення пеленгаційного рельєфу для лінійної антенної решітки з $N = 20$ на частоті $f = 1$ ГГц ($\lambda = 0,03$ м), що відповідає алгоритму Кейпона при наявності двох джерел випромінювання показано на рис. 1.

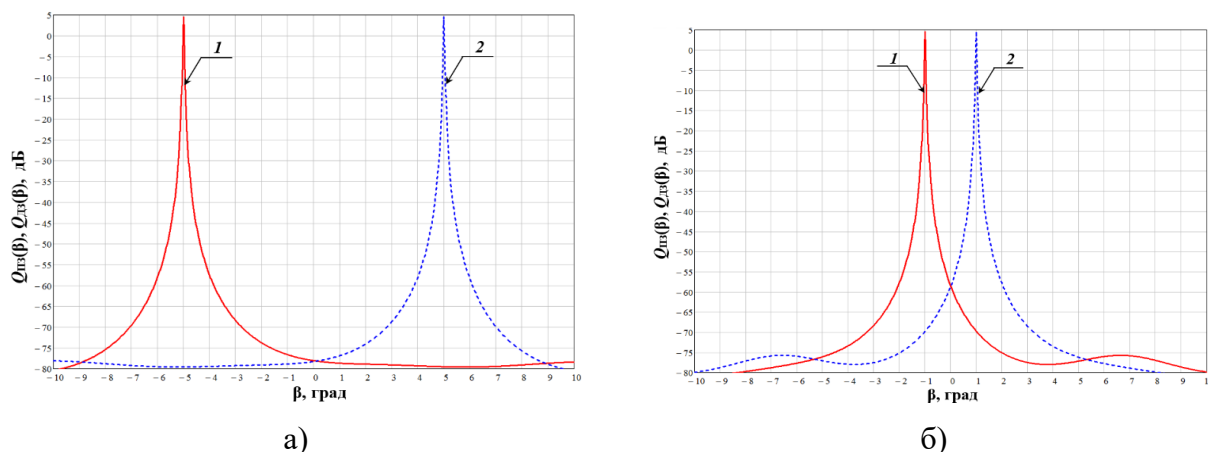


Рис. 1. Пеленгаційний рельєф при розташуванні двох джерел випромінювання: а) на пеленгах $\beta_1 = -5^\circ$, $\beta_2 = 5^\circ$; б) на пеленгах $\beta_1 = -1^\circ$, $\beta_2 = 1^\circ$.

Пеленгаційний рельєф отримується при скануванні вектором-гіпотезою деякого кутового сектора (одновимірного або двовимірного), що здійснюється в цифровій формі, із заміною істинної матриці R її максимально правдоподібною вибірковою оцінкою $\hat{R}$.

Отже, з безлічі алгоритмів пеленгації із надрозширенням найбільший інтерес, в загальному випадку, привертають алгоритми Кейпона і MUSIC, що застосовуються в антенних решітках будь-якої конфігурації – одновимірних, двовимірних і тривимірних, регулярних і не регулярних. Подальше удосконалення способів, алгоритмів та методів просторової обробки сигналів має свою доцільність та перспективність розвитку.

Література

1. Sukhov I. A. Super resolution techniques for direction-finder antenna array with directional elements / I. A. Sukhov, V. P. Akimov // Informatics. Telecommunications. Control / I. A. Sukhov, V. P. Akimov. – Saint Petersburg State Polytechnic University, 2013. – (Scientific and Technical Bulletin 4 ')). – С. 41–46.
2. Рембовский А.М., Ашихмин Л.В., Козьмин В.Л. Радиомониторинг: задачи, методы, средства/Под редакцией А.М. Рембовского. — М: Горячая линия-Телеком. 2006. 492 с.
3. Справочник по радиоконтролю. МСЭ 2002. — Женева. 2004.
4. Ратынский М. В. Адаптация и сверхразрешение в антенных решетках / М. : Радио и связь, 2003. — 197 с.
5. Кейпон Дж. Пространственно-временной спектральный анализ с высоким разрешением // ТИИЭР. 1969. Т. 57, № 8. С. 59-69.
6. Ратынский М.В. Анализ характеристик алгоритмов пеленгации со сверхразрешением // Радиотехника. 1992. № 10. С. 63 – 66.

КРИТЕРІЇ ОЦІНКИ ЕФЕКТИВНОСТІ РАДІОКАНАЛІВ МЕРЕЖ LTE

Скрябін С.А., Носков В.І.

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

CRITERIA FOR EVALUATION OF THE LTE NETWORKS RADIO CHANNELS EFFICIENCY

During the work the main key performance indicators of LTE mobile terrestrial networks which are used as part of or as performance evaluation criteria have been identified. The mathematical apparatus required for the analysis of the efficiency of radio channels is determined the mutual connection between the energy frequency and information criteria for evaluating the efficiency of the radio channels of the mobile terrestrial communication networks LTE is established.

В ході роботи були з'ясовані основні показники функціонування мереж мобільного наземного зв'язку LTE (Long Term Evolution), які використовуються в складі або в якості критеріїв оцінки ефективності радіоканалів. Визначений математичний апарат, потрібний для аналізу ефективності радіоканалів, встановлений взаємний зв'язок між енергетичним, частотним та інформаційним критеріями оцінки ефективності радіоканалів мереж мобільного наземного зв'язку LTE.

На даний момент мережі LTE використовуються досить широко. Швидкісні показники широкосмугової передачі даних у напрямках Downlink та Uplink свідчать про змogu даних мереж задовольняти різноманітні потреби користувачів: від передачі коротких повідомлень у месенджерах до контролю елементів автоматизованого виробництва автомобілів. Відповідно, постає задача оцінки та подальшого підвищення ефективності використання радіоканалів мереж LTE.

Оцінка ефективності функціонування радіоканалів мережі LTE може проводитися за трьома критеріями: енергетичним; частотним; інформаційним. Енергетичний критерій ефективності є збірним для групи показників ефективності функціонування підсистеми радіо доступу мереж 4G [1]. Фізичний зміст даного критерія ефективності радіоканалів визначає кількість енергії радіопередавача, що витрачається на передачу одного біту даних. Зменшення цього показника дозволить, наприклад, подовжити термін роботи абонентського пристрою на одній зарядці акумулятора. Зменшення потужності передавача в мережах 4G вирішується за рахунок функціонування закритої петлі контролю вихідної потужності передавача абонентського пристрою [2].

Закрита петля контролю вихідної потужності передавача абонентського терміналу представляє собою систему прийняття рішень, у якій абонентський термінал постійно проводить вимірювання енергетичних параметрів радіоканалу і надає базовій станції звіти по результатам вимірювань. Базова станція, в свою чергу, приймає рішення щодо потужності передавача абонентського пристрою. Абонентський пристрій вимірює декілька

енергетичних параметрів радіоканалів LTE [3], наведених нижче.

Потужність прийнятого опорного пілотного каналу - RSRP (Reference signal received power), яка визначається за формулою:

$$RSRP = \frac{RS_{CE}}{N},$$

де RS_{CE} – сума відліків потужності прийнятих каналних елементів, які переносять сигнал опорного пілотного каналу; N – кількість прийнятих каналних елементів, які переносять сигнал опорного пілотного каналу.

Якість прийнятого пілотного каналу, RSRQ (Reference signal received quality), яка визначається за формулою:

$$RSRQ = \frac{P_{RS}}{P_N},$$

де P_{RS} – потужність сигналу опорного пілотного каналу на вході приймача абонентського терміналу із урахуванням втрат на поширення радіохвиль; P_N – потужність шуму на вході приймача абонентського терміналу.

Відношення сигнал/шум плюс інтерференція, SINR (Signal to noise plus interference), яка визначається за формулою:

$$SINR = \frac{RSRP}{P_N + I},$$

де I – рівень інтерференції від сусідніх стільників.

За результатами цих вимірювань базовою станцією приймається рішення щодо необхідної потужності передавача абонентського терміналу [4].

Зазначені показники є визначальними у процесі функціонування підсистеми радіо доступу. У відповідності до цих параметрів не тільки задається рівень вихідної потужності передавача абонентського терміналу, а й схема модуляції. Наразі на мережах LTE найбільше поширення знайшли три види модуляції: QPSK, QAM16 та QAM64. Слід відзначити, що схема модуляції наряду пов'язана із таким критерієм ефективності радіоканалів як частотна або спектральна ефективність. Спектральна ефективність – це кількість біт інформації, які припадають на один герц наявного спектру. Міжнародним союзом електрозв'язку, а саме специфікацією ITU-R M.1801-2 чітко визначені параметри, у відповідності до яких треба використовувати ту чи іншу схему модуляції. Дані співставлення наведення у табл.1 [4].

Таблиця 1. Співставлення відношень сигнал/шум та схем модуляції для них.

Відношення SINR, дБ	Використовувана схема модуляції	Спектральна ефективність, біт/Гц
25	QAM-64	6
15	QAM-16	4
9	QPSK	2

Критерій інформаційної ефективності радіоканалів 4G визначає відношення реальної перепускної здатності до потенційної.

В мережах LTE використовується технологія передачі сигналів та множинного доступу OFDMA (Orthogonal frequency division multiple access). Дана технологія передбачає розподіл абонентів засобами частотно-часового

мультиплексування із ортогональними несучими сигналами. Структура фрагменту радіокадру OFDMA представлена на рисунку 1 [1].

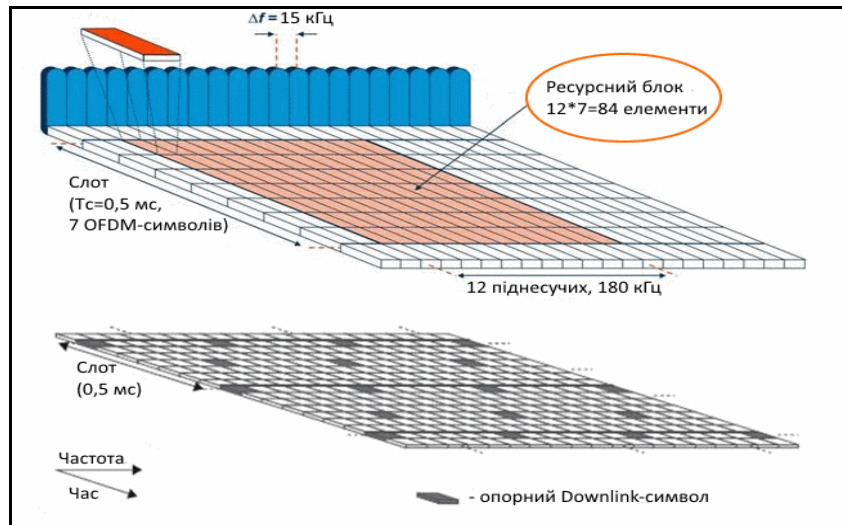


Рис. 1. Фрагмент радіо кадру OFDMA тривалістю 1 мс.

Тривалість одного радіо кадру складає 10 мс. Основу каналного ресурсу в рамках OFDMA складає ресурсний блок, який містить 12 частотних каналів, шириною 15 кГц кожний та 7 OFDMA – символів, розміщених у проміжку 0,5 мс. Ширина робочої смуги частот може варіюватися від 1,3 МГц до 20 МГц, залежно від наявного частотного ресурсу при розгортанні мережі LTE [2].

Міжнародним союзом електрозв'язку визначена формула для розрахунку пропускної здатності радіоканалу 4G, виражена співвідношенням [3]:

$$T = N_{MIMO} \times N_M \times N_{RE}|_{1мс},$$

де N_{MIMO} – використовувана конфігурація антенної системи MIMO; N_M – кількість інформаційних бітів на один герц частоти (спектральна ефективність); N_{RE} – кількість OFDMA – символів, які відповідають інтервалу в 1 мс при визначеній ширині смуги частот.

Підсумовуючи, слід зазначити, що критерії оцінки ефективності радіоканалів мереж мобільного наземного зв'язку пов'язані між собою і мають взаємний вплив. Практично неможливо оцінити ефективність використання радіоканалу за одним критерієм, бо в даному випадку має місце виключно комплексна оцінка ефективності за трьома основними критеріями. Задача оцінки та підвищення ефективності використання наявних для розгортання мереж LTE частотних каналів в залежності від різних факторів впливу є актуальною для подальших досліджень і аналізу.

Література

1. Скрыбін С.А. Технічні принципи побудови та протоколи функціонування підсистеми радіо доступу мережі мобільного зв'язку LTE: дипломна робота бакалавра телекомунікацій та радіотехніки: Київ, 2020, 83 с.
2. F. Mohammad LTE BIBLE – 2018 – Nokia Networks – 306 p.
3. C. Cox An Introduction to LTE – 2014 – John Wiley and Sons – 486 p.
4. ITU-R Specification M.1801-2.

СУЧАСНА ПРОБЛЕМАТИКА ІНТЕРНЕТУ РЕЧЕЙ

Міхненко Я.О., Курдеча В.В.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: yaroslavmikhnenko@gmail.com

MODERN PROBLEMS OF THE INTERNET OF THINGS

Despite the fact that the Internet of Things segment is currently experiencing a period of active growth, it seems that the world is still not ready to accept all the benefits of this concept. Potential customers lack specialists, investments and knowledge.

Незважаючи на те що сегмент «Інтернету речей» зараз переживає період активного росту, схоже, світ досі не готовий сприйняти всі переваги даної концепції. Потенційним замовникам не вистачає фахівців, інвестицій та знань.

Інтернет речей - це не тільки концепція; в її основі лежать цілком конкретні елементи і технології. Щоб внести більше ясності, перерахуємо основні з них.

По-перше, це сенсори і датчики – кінцеві пристрої IoT, збирають ті чи інші дані. Друга група, актуатори – також кінцеві пристрої, але вже мають вплив на навколишнє середовище, наприклад, освітлювальні прилади, електронні замки, динаміки і т.д.

Згадані елементи підключаються до шлюзів, які представляють собою спеціалізовані мікрокомп'ютери, здатні здійснювати первинний аналіз інформації від датчиків або давати певні команди актуаторами.

У масштабних системах шлюзи підключаються до повноцінних серверів (які відповідають за більш складну обробку і зберігання даних), а ті, в свою чергу, утворюють мережу або хмару.

Зв'язок між датчиками/актуаторами і шлюзами здійснюється за допомогою спеціалізованих енергоефективних технологій передачі даних, наприклад, LoRa або ZigBee. Шлюзи, в свою чергу, взаємодіють з серверами за класичними мереж Ethernet або Wi-Fi.

Коли тема «Інтернету речей» тільки починала розвиватися в широкому інформаційному полі, досить швидко намітилося два напрямки її розвитку - «важкі» корпоративні рішення і призначені для користувача системи. Прикладом першого з них є промисловий «Інтернет речей» (Industrial Internet of Things, IIoT), друга ж група об'єднує різну споживчу електроніку і рішення типу «розумний дім» (точніше навіть, «розумне житло»). Довгий час здавалося, що це два відносно незалежних напрямки, кожне з яких буде формувати окремий ринок, де за вигоду від використання унікальних технологій будуть платити, відповідно комерційні компанії і кінцеві споживачі. Зараз же стає все більш очевидним, що головним вигодонабувачем залишається бізнес, в першу чергу - великий. Одна з головних особливостей систем IoT - збір і аналіз детальної інформації - була

дуже доречною для багатьох компаній. У сучасному високо конкурентному світі бізнесу, особливо в економічно розвинених країнах, на ринку перемагає той, хто краще знає свого клієнта і враховує найдрібніші нюанси, що впливають на його вибір. Отримати таке знання можна за допомогою технологій IoT, збираючи інформацію з мільярдів призначених для користувача пристроїв - смартфонів, smart-годинників, побутових приладів, датчиків «розумного будинку» і т.д. При цьому кінцеві споживачі теж отримують певну перевагу у вигляді додаткових сервісів і зручностей, котрі забезпечує їм «розумна» споживча електроніка, але компанії набувають саме фінансову вигоду - то, що потім можна перетворити в гроші.

Але якщо компанії навчилися за допомогою «Інтернету речей» збирати дані і звертати їх собі на користь, значить, у них-то, швидше за все, справи йдуть чудово і за проектами IoT повинні буквально шикуватися черги замовників? У теорії начебто так, але, як завжди, хороші ідеї часто розбиваються об невблаганну практику. «Інтернет речей» - класичний приклад концепції, що обігнала свій час. Сьогодні у нас є маса підходів, ідей, навіть втілених розробок. Але не вистачає головного – універсальної інфраструктури передачі даних і єдиних стандартів. Домінуюча технологія також відсутня. Замість неї - десятки галузевих варіантів реалізації IoT. Логічно, що роль середовища передачі для основної маси пристроїв «Інтернету речей» повинні виконувати мережі операторів мобільного зв'язку, які охоплюють сьогодні більшу частину населення Землі. Але проблема в тому, що нинішні формати 3G і навіть 4G погано підходять для масового розгортання інфраструктур IoT - швидкості передачі даних повинні бути більші (рис 1.), а затримки менше. Скажімо, в США нормальної затримкою на мережах LTE вважається 50 мс - більш ніж достатньо для людського сприйняття, але в разі міжмашинних інтерфейсів, використовуваних пристроями IoT, бажано, щоб затримка була істотно менше - в межах декількох мілісекунд.

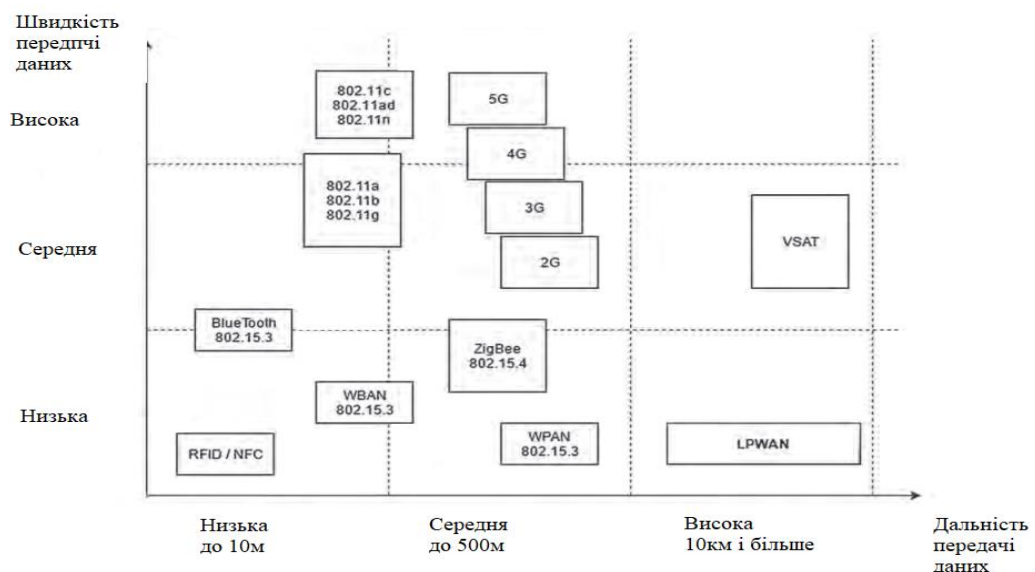


Рис. 1. Порівняння різних радіотехнологій, використовуваних для побудови мереж IoT.

Це можуть забезпечити тільки мобільні мережі п'ятого покоління (5G). Власне, з їх повсюдним впровадженням багато виробників пов'язують майбутній швидкий розвиток IoT, та й оператори по всьому світу так чи інакше розгорнуть 5G, як універсальну технологію передачі даних, в перспективі найближчих декількох років. Тому галузеві технології, наприклад, LPWAN, швидше за все будуть мати досить вузьке застосування, оскільки для них буде потрібно розгортати власні спеціалізовані мережі, замість того щоб використовувати вже готову інфраструктуру операторів зв'язку.

Ще одна проблема полягає в можливості масштабування. Класична ситуація - інженери розробляють відмінний проект, створюють прототипи і все працює, як задумано, поки мережа об'єднує всього кілька пристроїв. Коли ж проект швидко розростається і кількість підключень обчислюється тисячами, виникають несподівані технологічні проблеми, які просто неможливо було виявити на стадії прототипу.

Крім того, фахівці, що зіткнулися на практиці з великими проектами IoT, говорять про те, що складність подібних впроваджень зростає експоненціально, у міру підключення нових пристроїв. В результаті все більше часу починає йти на пошук помилок і налагодження процесів – в якийсь момент витрати на підтримку мережі IoT (як тимчасові, так і фінансові) починають перевершувати вкладення в її розвиток. Подібної ситуації сьогодні вдається уникнути, як правило, в тих проектах, де витриманий збалансований підхід до вимог функціональності та збору даних, іншими словами там, де обходяться розумним мінімумом того і іншого.

Судячи з усього, «Інтернет речей» чекає перспективне майбутнє. Адже ця концепція дуже вдало вбирає в себе всі самі передові технології. Поява 5G відкриває нові перспективи щодо розвитку інфраструктури IoT, інструменти роботи з великими даними дають можливість здійснювати глибокий і ефективний аналіз інформації, граничні обчислення (Edge Computing) дозволяють розвантажити дата-центри і магістральні канали зв'язку за рахунок локальних обчислень. Великі надії покладаються на майбутні досягнення в сфері штучного інтелекту, за допомогою якого вдасться забезпечити зручне управління мережами IoT і їх безшовне масштабування. Хмарні платформи стануть основою для обробки і надійного зберігання даних, а блокчейн забезпечить нові послуги з високим рівнем безпеки.

Література

1. IOT (ІНТЕРНЕТ РЕЧЕЙ): Детальний Аналіз [Електронний ресурс]. 201701. Режим доступу до ресурсу: <https://vkt.ua/articles/mnogogrannyj-internet-veshhej/>.
2. Overview of the Most Popular Smart Home Devices [Електронний ресурс]. 2019. Режим доступу до ресурсу: <http://iotlineup.com/>.
3. Порівняння різних радіотехнологій, що використовуються для побудови мереж IoT // <https://habr.com/ru/>.
4. Борецько О. Ю. Проектування IoT [Електронний ресурс] / Олег Юрійович Борецько. 2017. Режим доступу до ресурсу: <https://www.slideshare.net/ssuserf405bc/iot-79608563>.
5. Иванов К. Интернет вещей и безопасность: проблемы и решения [Електронний ресурс] / Константин Иванов. 2017. Режим доступу до ресурсу : <http://android.mobile-review.com/articles/49826/>.

АРХІТЕКТУРА MEC В МОБІЛЬНИХ МЕРЕЖАХ 4G

Правило В.В., Бірчин М.А.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: v.v.pravylo@ukr.net, mariana.birchyn143625@gmail.com

MEC ARCHITECTURE IN 4G MOBILE NETWORKS

The principle of building an ETSI MEC architecture, 4G MEC architecture. The main problems of 4G MEC are highlighted and their solutions are indicated.

З досягненнями в галузі мобільного Інтернету та безперервних появ різних служб і додатків, бездротові мережі спілкування зазнали вибухового зростання за минуле десятиліття.

Тому і зростають вимоги до цих мереж. Найскладніша вимога поставлена до латентності, яка впливає із взаємозв'язку тактильної дії людських кінцівок із зором або звуком, який становить близько мс.

MEC (Multi-access Edge Computing), яка запропонована ETSI (Інститут європейських стандартів телекомунікацій), може забезпечити можливості обчислювальної техніки та хмарних технологій для RAN, шляхом розгортання загальних ІТ-серверів на RAN (мережа радіодоступу), тим самим маючи наступні особливості:

- розвантаження трафіку, гнучка маршрутизація;
- локалізація послуг, кешування;
- вплив інформаційного контексту мережі;
- розвантаження обчислень.

ETSI MEC референтна архітектура. Як описано у визначенні, MEC може надавати ІТ та хмарні обчислювальні можливості для RAN шляхом розгортання загальних ІТ-серверів на межі RAN, на відміну від традиційної мережі, сервіси якої розміщені у віддаленому центрі обробки даних.

Як показано на рис. 1, клієнти програми або сторонні користувачі можуть взаємодіяти з системою MEC через системний рівень управління, який управляє життєвим циклом програми, правилами застосування та авторизацією послуг.

Існує три типи з'єднань, визначені між сутностями системи: з'єднання до функціональної платформи MEC (Mp), контрольні точки управління (Mm), контрольні точки, що підключаються до зовнішніх сутностей (Mx).

Хост MEC - це організація, що складається з платформи MEC та інфраструктури віртуалізації, яка забезпечує обчислення, зберігання та мережеві ресурси для додатків MEC.

Платформа MEC представляє колекцію базових функціональних можливостей, необхідних для запуску програм на певному хості MEC.

Інфраструктура віртуалізації включає площину даних, яка виконує правила пересилання, отримані платформою МЕС, та розвантаження трафіку до програми МЕС.

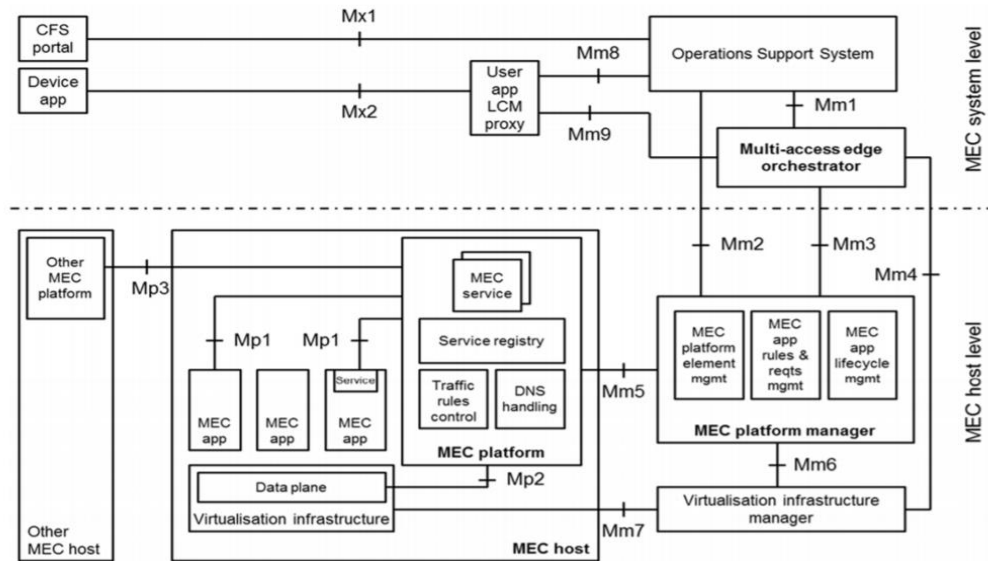


Рис.1. МЕС референтна архітектура.

Управління МЕС включає управління на рівні системи МЕС та управління рівнями МЕС.

Управління системним рівнем МЕС включає в себе основний компонент *Multi-access edge orchestrator*, який має огляд всієї системи МЕС.

Оскільки МЕС має намір створити стандартизоване і відкрите середовище для додатків та уникнення впливу на елементи мережі, що відповідають наявній 3GPP специфікації, ETSI в основному зосереджується на специфікації інтерфейсу MP1 між платформою МЕС і програмами та вимагає, щоб МЕС був прозорим для наявної реальної мережі 4G.

Це полегшує розгортання МЕС в реальній мережі, але спричиняє певні труднощі щодо експлуатації та обслуговування через відсутність мережевої підтримки.

Архітектура і проблеми 4G МЕС. Для того щоб уникнути зміни наявної мережі 4G, що вже розгорнута багато років, найважливішою вимогою є: МЕС повинна бути прозорою для реальної мережі.

Отже, перший крок розгортання МЕС у випробувальному процесі мережі 4G в основному фокусується на основній характеристиці трафіку – розвантаження.

Архітектура 4G МЕС

Рис.2 ілюструє запропоновану 4G архітектуру МЕС на основі мережевої архітектури LTE, в яку МЕС вставляється між CN (основна мережа) та RAN.

Щодо трафіку, що протікає через МЕС, вони будуть оброблятися по-різному, що включає контроль сигналізування, трафік висхідної та низхідної лінії зв'язку.

Детальний спосіб розвантаження трафіку буде описано наступним чином:

1) *Сигналізування площини управління*: МЕС направить контроль сигналізування до ММЕ прозоро. Це для того, щоб отримати TEID користувача (ідентифікація тунелю), яка відповідає за ідентифікацію користувачів у протоколі GTP і є дуже важливою для переадресації трафіку висхідної лінії локальної служби до конкретного користувача.

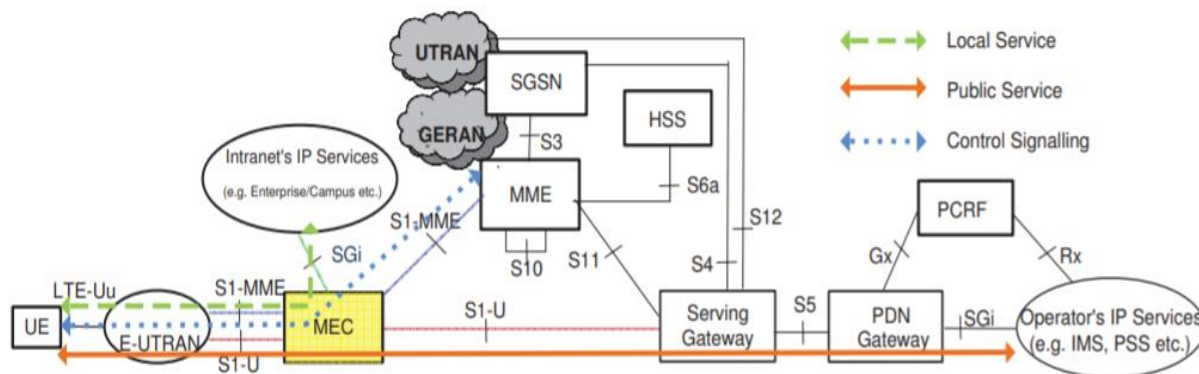


Рис.2. 4G MEC-архітектура.

2) *Трафік висхідної лінії зв'язку на площині користувача*:

- Public Service: МЕС перенаправлятиме трафік до S-GW (Serving Gateway) прозоро без будь-якої обробки.

- Local Service: МЕС придбає IP-адресу (джерело і пункт призначення) та номер порту шляхом декапсуляції GTP (GPRS Tunneling Protocol) PDU, а потім розвантажить трафік до локальної мережі.

3) *Трафік низхідної лінії зв'язку на площині користувача*:

- Public Service: МЕС перенаправлятиме трафік до eNB прозоро без будь-якої обробки.

- Local Service: МЕС інкапсулює IP PDU в GTP PDU використовуючи TEID користувача, отриманий в результаті аналізу контрольного сигналізування, а потім переадресує GTP PDU на eNB.

Проблеми 4G МЕС. На основі польових випробувань 4G МЕС було виявлено, що ще потрібно вирішити деякі проблеми для подальшого просування, такі як:

- функція обходу МЕС;
- проблема безпеки.

Можна зробити висновок, що хоча МЕС є привабливою технологією для мобільної мережі, але для її комерційного розгортання і для роботи в мережі 4G все ще потрібно більше роботи в польових умовах.

Література

1. Residential CORD.[<https://www.etsi.org/technologies/multi-access-edge-computing>].
2. https://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/02.02.01_60/gs_MEC003v020201p.pdf
3. Dario Sabella, Alex Reznik, Rui Frazao Multi-Access Edge Computing in Actijn // 2019.
4. Enterprise CORD. <https://link.springer.com/article/10.1007/s00521-020-05267-x#Bib1>, 2020.

АНАЛІЗ ЗАВАДОЗАХИЩЕНОСТІ ПРОЦЕСУ ВХОДЖЕННЯ В СИНХРОНІЗМ РАДІОЛІНІЇ УПРАВЛІННЯ БПЛА З ППРЧ

Василенко С.В.

*Інститут спеціального зв'язку та захисту інформації
Національний технічний університет України "Київський
політехнічний інститут імені Ігоря Сікорського", Україна
E-mail: vasylenko.phd@gmail.com*

ANALYSIS OF THE SYNCHRONISM ENTERING PROCESS ROBUSTNESS IN UAV'S RADIO CONTROL LINE WITH FHSS

In the work, on the basis of the developed simulation model of the entering into synchronism process of the unmanned aerial vehicle (UAV) control line with the frequency-hopping spread spectrum (FHSS), a number of experiments and estimation of the entering into the synchronism process noise immunity of the UAV control line with the FHSS under conditions of powerful intentional interference.

Обмежені можливості застосування безпілотних літальних апаратів (БПЛА) в складних радіоелектронних умовах та невинне зростання питомої ваги завад в умовах обмеженості радіочастотного ресурсу обумовили доцільність застосування в системах управління БПЛА широкосмугових сигналів з псевдовипадковим переналаштуванням робочої частоти (ППРЧ).

Велика кількість робіт присвячена питанню розкриття властивостей методу ППРЧ та методики формування сигналів з ППРЧ в умовах впливу навмисних та ненавмисних завад [1-3]. У даних роботах детально розглядаються переваги та недоліки зазначеного методу, представлені основні математичні моделі системи радіозв'язку з ППРЧ та проводиться аналіз завадозахищеності зазначеного методу. Проте у даних роботах не достатньо уваги приділяють завадозахищеності процесу входження в синхронізм. Аналіз [4] показав, що на етапі пошуку складного сигналу з ППРЧ завадозахищеність радіолінії характеризується завадозахищеністю алгоритму входження в синхронізм.

В роботі на основі відомої методики оцінки завадозахищеності алгоритму входження в синхронізм радіолінії з ППРЧ [5] та синтезованої математичної моделі процесу входження в синхронізм радіолінії управління БПЛА з ППРЧ [6] в середовищі комп'ютерного моделювання Matlab R2017a з пакетом розширення Simulink розроблено імітаційну модель (ІМ) процесу входження в синхронізм радіолінії управління БПЛА з ППРЧ (рис. 1).

У розробленій ІМ на вході передавача формується дві послідовності Касамі, що містять інформацію про номер частоти та номер підциклу передавача (синхромітка), та блок службової інформації, що закодована за допомогою мажоритарного кодування. Сформована синхромітка та блок службової інформації об'єднуються в синхрокадр, який після перемноження зі спільною (завчасно відомою обом користувачам) псевдовипадковою

послідовністю (ПВП), надходить на вхід BPSK-модулятора. Після модуляції сформований синхрокадр передається у AWGN-канал, де піддається впливу навмисної завади противника. Для імітації впливу противника в роботі використовується генератор випадкових двійкових чисел Бернуллі.

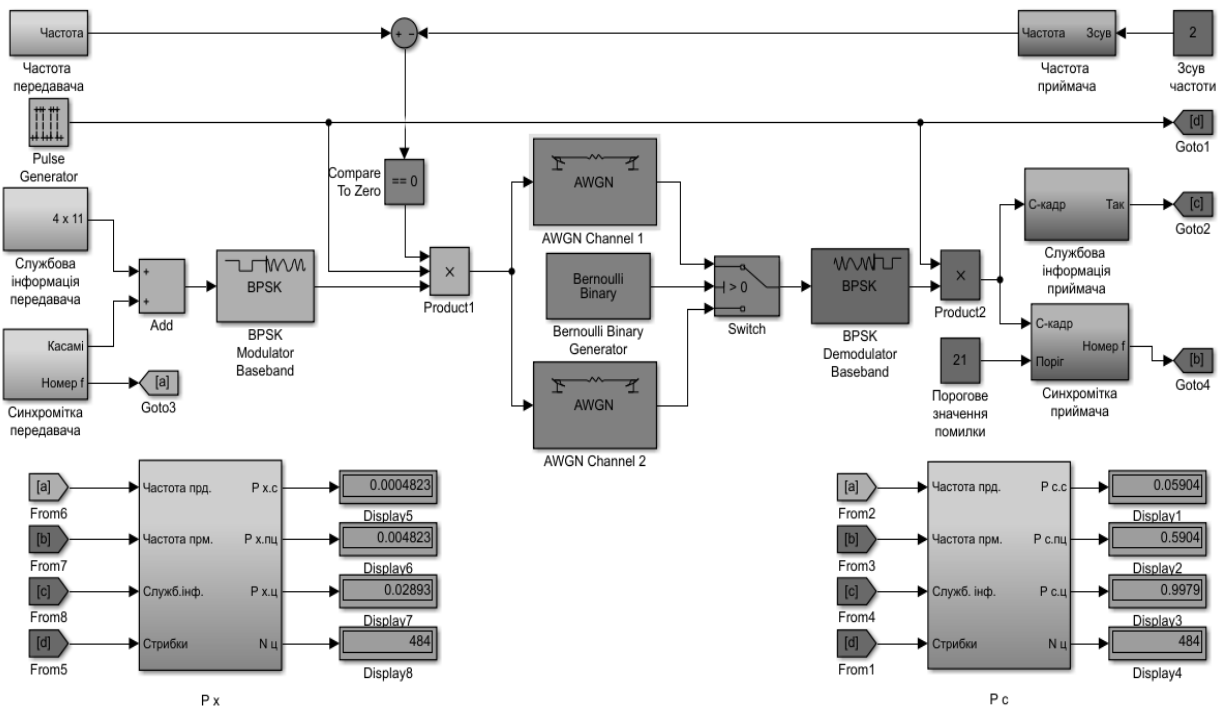


Рис. 1. Структурна схема ІМ.

Оскільки методика [5] передбачає, що не всі частоти входження в синхронізм уражені навмисною завадою, для імітації середовища розповсюдження використовується два AWGN-канали. У випадку, коли частота не уражена, сигнал проходить через канал зі значним рівнем шуму (AWGN Channel 1). Якщо ж ураження частоти навмисною завадою відбулося, то за допомогою ключа (Switch) здійснюється переключення на іншу лінію (AWGN Channel 2), де потужність сигналу значно перевищує потужність шуму.

Прийнятий сигнал передавача, за допомогою BPSK-демодулятора, демодулюється та перемножується на спільну ПВП. Після цього відбувається виділення з синхрокадру синхромітки та блоку службової інформації.

Рішення про правильність прийому синхрокадру, а отже і входження в синхронізм, на приймальній стороні приймається на основі порівняння отриманих послідовностей Касамі з власними.

Для проведення оцінки статистичних даних в ІМ використовуються блок оцінки ймовірності вірного (P_c) та хибного (P_x) входження в синхронізм, що дозволяють проводити аналіз ймовірностей входження в синхронізм за одну частотну позицію (стрибок), підцикл та цикл передачі.

За допомогою розробленої ІМ проведено аналіз залежності ймовірності вірного ($P_{c.ц}$) та хибного ($P_{x.ц}$) входження в синхронізм за один цикл передачі радіолінії управління БПЛА з ППРЧ для різних значень відношення потужності сигнал/шум на уражених (SNR_+) та неуражених (SNR_-) частотах

від значень, що характеризують завадову обстановку ($P_{\text{ураж}}$). Значення SNR_+ , SNR_- та $P_{\text{ураж}}$ задаються на початку експерименту.

Проведений аналіз результатів моделювання показав, що при значеннях $SNR_+ = -10$ дБ, $SNR_- = -5$ дБ та $P_{\text{ураж}} = 0,4$ ймовірність вірного входження в синхронізм наближається до 1 ($P_{\text{с.ц.}} = 0,996$). При погіршені завадової обстановки до $P_{\text{ураж}} = 0,6$ та зменшенні значення SNR_- до -10 дБ ймовірність входження в синхронізм знижується і складає $P_{\text{с.ц.}} = 0,7$.

Значення ймовірності хибної синхронізації, для вище розглянутих випадків, є незначними та знаходиться в межах $P_{\text{х.ц.}} = [0,0195; 0,0245]$.

Розроблена ІМ процесу входження в синхронізм радіолінії управління БПЛА з ППРЧ дозволяє:

- перевірити працездатність синтезованої математичної моделі процесу входження в синхронізм радіолінії управління БПЛА з ППРЧ;
- провести низку експериментів для різних значень завадової обстановки в якій змушений працювати БПЛА;
- оцінити завадозахищеність процесу входження в синхронізм радіолінії управління БПЛА з ППРЧ.

ІМ також дозволяє проводити вибір необхідних параметрів алгоритму входження в синхронізм для досягнення максимального рівня завадозахищеності процесу входження в синхронізм радіолінії з ППРЧ.

Розроблена ІМ є уніфікованою та може бути використана при розробці нових чи модернізації відомих засобів радіозв'язку з ППРЧ.

Література

1. Чуднов А. М. Об адаптивных алгоритмах псевдослучайного переключения рабочих частот радиолиний в условиях случайных и преднамеренных помех. *Журнал радиоэлектроник*. 2015. № 4.
2. Fernández de Gorostiza E., Berzosa J., Mabe J., Cortiñas R. A Method for Dynamically Selecting the Best Frequency Hopping Technique in Industrial Wireless Sensor Network Applications. *Sensors*. 2018. Vol. 18, Issue 2. P. 657. doi: <https://doi.org/10.3390/s18020657>.
3. Гурський Т. Г., Кривенко О. В. Методика формування сигналу в радіозасобах з ППРЧ при передачі мови в умовах впливу завад у відповідь. *Системи управління, навігації та зв'язку*. 2017. № 2. С. 179 – 184.
4. Березюк М. В. Завадозахищеність синхронізації радіолінії з ППРЧ та фіксованим набором частот входження. *Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення* : зб. мат. IV наук.-практ. семін. Київ : ВІТІ НТУУ “КПІ”, 2007. С. 58.
5. Міщенко В. Г., Єрохін В. Ф. Методика оцінки завадозахищеності алгоритмів входження в синхронізм радіолінії з псевдовипадковим перелаштуванням радіочастоти. *Захист інформації*. 2001. № 2. С. 32 – 59.
6. Рома О. М., Василенко С. В. Вибір параметрів алгоритму входження в синхронізм радіолінії управління безпілотним літальним апаратом з псевдовипадковим перелаштуванням робочої частоти. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*. 2016. № 54. С. 71 – 78.

ВДОСКОНАЛЕНА МОДЕЛЬ БЕЗПЕКИ 5G**Кормульов О. С.***Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна**E-mail: steallex214@gmail.com***ENHANCED 5G SECURITY MODEL**

This article introduces an improved 5G security model to help secure networks against all kinds of attacks and threats. Its main elements and characteristics are described in detail. The security features of 5G networks, its dependence on various factors have been investigated as well.

Висока швидкість 5G відкриває величезне поле можливостей: нові види послуг, сервісів та цілі бізнес-моделі, які здавалися неможливими в мережах минулих поколінь. До переваг 5G в порівнянні з мережами минулих поколінь можна віднести можливість підключення великої кількості пристроїв, високу енергоефективність, високу мобільність користувачів; в декілька разів зросла пропускна здатність, яка дозволяє забезпечити більшу доступність широкосмислового мобільного зв'язку.

Але з новими перевагами та плюсами, новими системами з'являться і нові вразливі місця. Для захисту 5G від вдосконалених і складних видів загроз потрібна розвинена модель безпеки (яка зображена на рис. 1.), яка пропонує глибокий захист не тільки від існуючих, але і від еволюціонуючих та нових видів загроз, а також загроз нульового дня. Це вимагатиме чітко визначеної стратегії безпеки та плану захисту різних компонентів для мережі 5G, включаючи кінцеві пристрої та кінцевих користувачів. Ефективна стратегія безпеки може бути розроблена на основі телеметричних даних, отриманих за допомогою добре розробленої системи спостереження. Необхідно визначити процеси та інструменти для участі у виявленні атак та нападів на систему, блокувати їх та розвивати систему захисту мережі.

Забезпечення належного рівня безпеки є обов'язковим для видів загроз які постійно змінюються та атак на системи безпеки 5G мереж. Для посилення безпеки та захисту даних користувачів, модель безпеки має відповідати наступним вимогам та параметрам:

1) *Конфіденційність*: в моделі безпеки 5G конфіденційність даних є однією з основних вимог безпеки; властивість, яка може захистити передачу даних від розголошення її стороннім особам та від пасивних атак (тобто, прослуховування та підслуховування). Враховуючи архітектури 4G-LTE та 5G, будь-які дані користувача повинні бути конфіденційними та захищеними від несанкціонованих користувачів. Стандартні алгоритми шифрування даних широко прийняті для реалізації конфіденційності даних у мережевих додатках 5G (наприклад, мережах транспортних засобів, моніторингу стану здоров'я тощо). Симетричні криптосистеми можуть бути використані для шифрування та дешифрування даних 5G одним і тим же приватним

криптографічним ключем. Вони обмінюються між комунікаційними об'єктами (наприклад, відправником та одержувачем).



Рис. 1. Посилена модель безпеки 5G розпізнавання загроз.

Симетричні криптосистеми можуть бути використані для шифрування та дешифрування даних 5G одним і тим же приватним криптографічним ключем. Вони обмінюються між комунікаційними об'єктами (наприклад, відправником та одержувачем).

2) *Цілісність*: запобігання втручанню та втраті інформації під час її переміщення з однієї точки в іншу. Цілісність даних в 5G NR захищена аналогічно 4G. У 5G NR цілісність захищена бездротовим трафіком даних на рівні протоколу конвергенції пакетних даних (PDCP). У 4G LTE захищеність цілісності забезпечується лише для шару (рівня) без доступу (NAS) та шару доступу (AS). Однак однією з головних відмін у захисті цілісності 5G є те, що 5G NR також забезпечує захист цілісності площини користувача. Це важливо, оскільки в 4G такої функції не було. Ця нова функція корисна для невеликих передач даних, особливо для обмежених пристроїв IoT. Більше того, механізм аутентифікації 5G 5G-AKA використовує захищену телесигналізацію. Це гарантує, що жодна сторона, яка не має права, не може змінювати та отримувати доступ до інформації, яка передається в ефірі.

3) *Доступність*: у області 5G доступність мереж - це забезпечення доступності мережевих ресурсів тоді, коли вони будуть потрібні законним користувачам, оскільки доступність впливає на репутацію постачальника послуг. Іншими словами, доступність забезпечує високу ймовірність ефективності мережевої інфраструктури. Вона також вимірює стійкість мережі проти активних атак, наприклад, DoS-атак. Атака DoS може погіршити продуктивність мережі. Однак за допомогою надширокосмугового мобільного зв'язку (eMBB) та надвисокого надійного MachineType-зв'язку

(uMTC) доступність мережі може бути досягнута як мінімум на 95% та 99,99% відповідно, при їх застосуванні в 5G мережі.

4) *Централізована політика безпеки*: архітектури безпеки 3GPP 4G не можуть безпосередньо застосовуватися для використання в мережах 5G, оскільки вони присвячені традиційній моделі довіри оператор-абонент. Тому для підтримки нових інновацій (таких як NFV та SDN) існує потреба у централізованій системі управління політикою безпеки, яка забезпечує зручність доступу користувачів до додатків та ресурсів. Для цього можна використовувати структуру управління безпекою на основі політик (policy-based) для підтримки централізованого управління безпекою для 5G. Цей метод полягає в тому, що він використовується для прийняття рішень з проблемами безпеки на основі політик, встановленими адміністратором мережі, або оператором. Крім того, оператори можуть включити Security-as-a-Service (SaaS) як потенційне рішення проблем з безпекою для ряду клієнтів.

5) *Видимість*: дозволяє ефективно вирішити основні проблеми мережі для забезпечення безпечного середовища. Мережам 5G необхідно використовувати комплексні стратегії наскрізного (end-to-end) захисту які повинні охоплювати всі рівні мережі. Для реалізації такого всебічного механізму безпеки 5G-оператори повинні мати повну видимість, перевірку та контроль над усіма рівнями мережі. Технології 5G повинні бути інтегровані з відкритими API для управління політикою безпеки.

Таким чином, мережа 5G може мати послідовну політику безпеки як програмного, так і апаратного забезпечення в мережі. Покращена видимість всієї мережі та політик безпеки допоможуть реалізувати нові посилені механізми безпеки, що підходить для нових послуг 5G. Більше того, покращення видимості дозволяє запобігти загрозам, що керують даними, знаходити та ізолювати заражені пристрої до того, як вони вчинили атаку на мережу.

У роботі представлено вдосконалену модель безпеки 5G, яка допомагає захистити мережі від будь-яких видів атак та загроз. Детально описано та зображено її основні елементи, вимоги, параметри та характеристики. Також досліджено особливості безпеки мереж 5G, її залежність від різноманітних факторів. Проблеми безпеки та конфіденційності зв'язку будуть більш помітні, коли до 5G мереж буде підключено більше користувачів. Врахування цих можливих загроз від початкових етапів проектування до розгортання самих мереж 5G зведе до мінімуму ймовірність можливих помилок безпеки та конфіденційності.

Література

1. A Comprehensive Guide to 5G Security / Madhusanka Liyanage; Ijaz Ahmad; Ahmed Bux Abro; Andrei Gurtov; Mika Ylianttila, 1st Edition вид. Helsinki, Finland: Kindle Edition, 2017.
2. Ijaz Ahmad. Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, Andrei Gurtov 5G security: Analysis of threats and solutions // 2017 IEEE Conference on Standards for Communications and Networking (CSCN). Helsinki, Finland: 2017.
3. 5G Security White Paper // Huawei. 2019.

ТЕХНОЛОГІЯ 5G І ЇЇ ВПЛИВ НА ІНТЕРНЕТ РЕЧЕЙ

Правило В. В., Хижняк О. П.

Інститут телекомунікаційних систем КІП ім. Ігоря Сікорського, Україна

E-mail: v.v.pravylo@ukr.net, hiz01072000alex@gmail.com

FIFTH GENERATION TECHNOLOGY AND ITS IMPACT ON THE INTERNET OF THINGS

The technology of 5g in combination with IoT is considered. Problems and their solutions are covered through the introduction of 5th generation mobile technology in the field of smart home and IoT in general.

Науково-технічний прогрес не стоїть на місці і проявляється не тільки в тому, що в побуті з'являються нові девайси, датчики, гаджети і програмне забезпечення до них, але ще напевно важливіше те, що вони розширюють можливості людей. Аналітична компанія Strategy Analytics представила результати дослідження світового ринку обладнання в сфері Інтернету речей (IoT) [1]. Відповідних пристроїв наприкінці 2018 року вже налічувалось більше 20 млрд штук, якщо подивитися на тенденцію зростання з кожним роком, то можна прогнозувати, що на 2022 рік цифра зросте до 30 млрд штук (див. рис. 1), більша частина - понад 50% - з них доводиться на корпоративний сектор. Частка мобільних і обчислювальних пристроїв в загальному обсязі даного ринку склала трохи більше 25%. Однак сегментом який найшвидше зростає в найближчі роки повинна стати побутова електроніка багато в чому завдяки популяризації систем «розумного будинку».



Рис. 1. Кількість підключених пристроїв до інтернету.

Наші будинки вже наповнені підключеними пристроями. Крім телефонів, планшетів і комп'ютерів, телевізори або телевізійні приставки, можливо, також використовують Інтернет, на ньому зав'язані майже всі функції інтелектуальної динаміки на кухні, а ваш розумний термостат

втрачає всі дані, якщо припиняє працювати Wi-Fi. Це вже створює значні навантаження на домашню мережу, особливо коли відразу кілька людей намагаються нею користуватися. А якщо включені кілька пристроїв, проблема лише поглиблюється [2].

Для пристроїв розумного будинку ненадійне з'єднання, яке може перериватися створює реальну проблему з точки зору як загальних параметрів роботи, так і сприйняття користувачами ефективності продукції. Якщо світлові прилади з голосовою активацією відразу не спрацювали і людина залишилася стояти в темряві, у нього швидко пропаде бажання користуватися нібито футуристичними новими гаджетами.

Сьогоднішня продукція розумного будинку покладається на різні стандарти зв'язку, але всі вони вимагають підключення до домашньої мережі. Однак можливості збільшення діапазону і швидкості Wi-Fi обмежені, особливо коли маршрутизатор потрібно встановити біля телефонної розетки. Підлоги, стіни і двері можуть негативно впливати на роботу мережі. Інші бездротові сигнали, конкуруючі за пропускну здатність мережі, також можуть погіршити ситуацію.

Збільшення максимальної швидкості і пропускну здатності мережі може допомогти лише трохи, особливо в зонах низької швидкості широкосмугового доступу, а здатність 5G забезпечувати енергоефективну мережу дальнього радіусу дії (LPWAN) ідеально підходить для експлуатації продукції розумних будинків, що вимагає постійного надійного підключення. Велика пропускну здатність 5G також означає можливість підключення набагато більшого числа пристроїв в порівнянні з локальною мережею. Також це означає, що будинкам більше не знадобиться дротова інфраструктура, модернізація якої затратна і незручна, особливо в сільській місцевості.

Єдиний універсальний стандарт безпроводного підключення також допоможе вирішити одну з головних проблем сучасних пристроїв: відсутність сумісності. Якщо всі пристрої будуть використовувати однаковий протокол зв'язку, їх взаємодія покращиться, що в цілому позитивно позначиться на екосистемі розумного будинку.

За допомогою технології 5G сфера IoT, та загалом розумний будинок отримає безліч переваг. Одною з найбільших комерційних переваг є низький рівень затримок. У нинішніх пристроїв розумних будинків відповідь на сигнали і команди займає кілька секунд, що не так вже й багато. Але затримка вже стане помітною при використанні голосових команд, а для підключених пристроїв безпеки, наприклад камер і ламп, це буде мати велике значення. Чим швидше вони реагують і попереджають вас про вторгнення, тим більша ймовірність, що вони відлякують зловмисника. Наприклад, у 4G затримка сигналу становить близько 40 мілісекунд. У мереж п'ятого покоління затримка в ідеалі становить одну мілісекунду [3] і не перевищує п'яти - різниця з 4G мінімум у вісім разів, та якщо ми говоримо про IoT, то

наприклад, якщо взяти сферу безпілотних авто, то середній час реакції людини на візуальний стимул становить 250 мс або 1/4 секунди. Уявіть собі, що ваша машина може реагувати в 250 разів швидше, ніж ви [4].

І це не єдиний варіант, коли 5G може допомогти вам підвищити рівень безпеки. Пристрої розумного будинку сумно відомі тим, що є слабкою ланкою для проникнення хакерів, але технологія 5G використовує більш складний рівень шифрування: 256-бітове в порівнянні з 128-бітовим у 4G.

П'яте покоління стільникового зв'язку також полегшить використання переносних датчиків для контролю стану здоров'я і самопочуття вразливих членів суспільства, дозволяючи медичним працівникам використовувати пристрої телеприсутності для спілкування і надання допомоги пацієнтам, які не можуть або яким заборонено здійснювати поїздки.

Основні атрибути 5G включають [4]:

1. Значно більш високу швидкість передачі даних, ніж 2G, 3G, 4G. У мережах п'ятого покоління пікова швидкість в 20 разів вище, ніж у попередника. Швидкість передачі може досягати 15 або 20 Гбіт / с.

2. Підтримка масових машинних комунікацій, при яких велика кількість машин або пристроїв обмінюється даними без будь-якої людської взаємодії або контролю.

3. Затримка - це час, необхідний для відправки даних з пристрою в мережу і назад, та у технології 5G її мінімізували до 1 мілісекунди.

4. Щільність підключення до одного мільйона з'єднань на квадратний кілометр. Це особливо важливо в той час, коли Інтернет речей швидко розширюється. Можна розмістити більше датчиків, активаторів, предметів і пристроїв без значного впливу на швидкість мобільного Інтернету.

5. Мережі 5G зможуть працювати з малопотужними пристроями інтернету речей. Безліч мікродатчиків і сенсорів будуть служити автономно місяцями без зміни або підзарядки батареї живлення. Це важливо, тому що забезпечити мільйони IoT-пристроїв доступом до електромережі було б вкрай складним інженерним завданням, часто зовсім не розв'язуваним: вона б звела нанівець всі плюси від виникнення інтернету речей.

Отже, швидкість, пропускна здатність, низький рівень затримок і повсюдне поширення 5G здатні впоратися з проблемами, які були розглянуті, і поліпшити всі аспекти: від безпеки до загальної продуктивності пристроїв розумного будинку.

Література

1. У світі підраховано кількість IoT-пристроїв [<http://www.dailycomm.ru/m/47373/>].
2. Як 5G зробить ваш будинок розумнішим [<https://www.intel.ru/content/www/ru/ru/it-managers/5g-smart-home.html>].
3. 5G – Wikipedia [<https://ru.wikipedia.org/wiki/5G>].
4. Introducing 5G technology and networks [[https://www.thalesgroup.com/en/markets/digital-identity-and-security/mobile/inspired/5G#:~:text=5G%20technology%20offers%20an%20extremely,millisecond\(1ms\)%20with%205G](https://www.thalesgroup.com/en/markets/digital-identity-and-security/mobile/inspired/5G#:~:text=5G%20technology%20offers%20an%20extremely,millisecond(1ms)%20with%205G)].

ПАРАМЕТРИ ОЦІНКИ ЯКОСТІ ГОЛОСОВОГО ТРАФІКУ В МЕРЕЖАХ LTE

Ветошко І.П., Носков В.І.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: ivan.vetoshko@ukr.net

QUALITY EVALUATION PARAMETERS FOR VOICE TRAFFIC IN THE LTE NETWORK

During the work, the quality evaluation parameters for voice traffic in the LTE network were considered. The principle of QoS quality performance distribution in the IMS subsystem as well as approaches for end-to-end voice quality evaluation were defined.

В ході роботи було розглянуто параметри оцінки якості голосового трафіку в мережі LTE. Приведено принцип розподілу якісних показників обслуговування QoS в підсистемі IMS та визначено підходи до оцінки якості наскрізної передачі голосу.

На сьогоднішній день, швидке розгортання мереж LTE і високий рівень проникнення смартфонів створило проблему для операторів мобільних мереж, котра полягає в цілковитій структурі мережі LTE на основі IP, яка не може підтримувати передачу традиційних голосових послуг. Тому оператори мобільного зв'язку активно виконують міграцію голосового трафіку в мережі з комутацією пакетів. Концепція архітектури LTE передбачає застосування додаткової підсистеми IMS (IP-Multimedia Subsystem), що виконує головну роль в організації голосових сесій абонентів. Важливою вимогою до передачі голосу є висока якість надання послуги [1].

В мережах LTE за рахунок використання підсистеми IMS впроваджена технологія передачі голосу VoLTE (Voice over LTE). Технологія VoLTE - це рішення для передачі голосових пакетів в мережі LTE з малою затримкою і високим рівнем якості обслуговування. Мобільні мережі LTE в змозі надавати наскрізні (E2E - End-to-End) послуги високої чіткості (High Definition, HD) операторського класу з гарантією обслуговування. Ці послуги можуть сприяти підвищенню конкурентоспроможності провайдерів з постачальниками OTT (Over the Top) сервісів [2]. Це стосується і голосового трафіку.

Відомо, що потік пакетів голосового трафіку є дуже чутливим до характеристик передачі, таких як затримка та джитер затримки. Для забезпечення якості, в мережах четвертого покоління передбачена підтримка QoS (Quality of Service), що реалізується через поділення всіх видів послуг на 9 класів. Кожному класу призначається ідентифікатор QCI (QoS Class Identifier). В свою чергу, наскрізні канали для передачі трафіку поділені на дві групи в залежності від типу виділеного ресурсу, а саме: з гарантованою швидкістю передачі (Guaranteed Bit Rate, GBR) та з негарантованою швидкістю передачі Non-GBR. В табл. 1 наведено якісні показники для

основних видів надання послуг в мережах LTE.

Для того, щоб організувати якісну передачу голосового трафіку за технологією VoLTE потрібна підтримка двох QCI: 1 та 5. Ідентифікатор 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. Через з'єднання по QCI 1 голосові дані передаються з використанням стека протоколів RTP/UDP/IP [3].

Таблиця 1. Якість обслуговування в мережах LTE.

QCI	Тип	Пріоритет	Допустима затримка, мс	Допустимі втрати	Приклад
1	GBR	2	100	10^{-2}	VoLTE виклик
2		4	150	10^{-3}	Відео виклик
3		5	300	10^{-6}	Онлайн ігри
4		3	50	10^{-3}	«Стрім» відео
5	Non-GBR	1	100	10^{-6}	IMS
6		7	100	10^{-3}	Електронна пошта, чат
7		6	300	10^{-6}	Голосові, відео, інтерактивні ігри
8		8	300	10^{-6}	Електронна пошта, чат

Параметрами якості наскрізного з'єднання в мережі LTE є параметри, що ґрунтуються на сприйнятті послуги кінцевими користувачами, а також параметри, які визначають якість передачі пакетів в мережі [4] :

- **Коефіцієнт успішності реєстрації** – інтенсивність успішних спроб реєстрації в службі VoLTE;
- **Готовність служби**, тобто можливість встановлення наскрізного з'єднання між клієнтами мережі VoLTE;
- **Коефіцієнт ефективності мережі**, що визначає здатність мережі доставляти виклики клієнту VoLTE з точки зору сервісної платформи;
- **Інтенсивність помилок мережі (NER – Network Error Ratio);**
- **Коефіцієнт ефективності встановлення сеансів зв'язку (SEER);**
- **Затримка після набору номера**, тобто інтервал часу (в секундах) між закінченням набору номера абонентом та прийомом ним відповідного тонального сигналу виклику або записаного оголошення;
- **Середня експертна оцінка якості мовного повідомлення (Mean Opinion Score, MOS)**, що визначається суб'єктивним сприйняттям голосового повідомлення клієнтами. Даний параметр може визначатися для кожного виклику або вибірково;
- **Затримка від клієнта-джерела голосового повідомлення до клієнта-слухача** – це час, необхідний для передачі мовного сигналу між

клієнтами. Він може змінюватися від 150 мс до максимум 400 мс;

- **Коефіцієнт перерваних з'єднань** – це безперервність обслуговування щодо здатності підтримувати з'єднання до їх нормального завершення;
- **Смуга пропускання мовного сигналу (NB – Narrow Band, WB – Wide Band або SWB – Super Wide Band)** – це міра використовуваної смуги пропускання.

Показники якості продуктивності (Key Performance Indicator, KPI) QoS VoLTE обчислюються шляхом порівняння якості передачі реальних пакетів трафіку VoLTE з стандартними опорними значеннями та зі значеннями, що одержані в результаті попередніх досліджень за допомогою моделювання.

Існує два підходи до оцінки якості наскрізної передачі голосу:

- **Параметричні інструменти** - використовують хорошу кореляцію між технічною інформацією про з'єднання і відповідною якістю наскрізної передачі. Такий інструмент доцільно впроваджувати в прикордонних точках, близьких до кінцевих користувачів;
- **Сигнальні моделі** - набагато складніші параметричних інструментів, оскільки вони вимагають введення і аналізу мовного сигналу. Тому їх в основному використовують в ракурсі точка - точка для точного вимірювання якості наскрізної передачі голосу в даний момент часу і в певному місці [5].

Підсумовуючи, можна сказати, що якість передачі мовного сигналу в мережі LTE визначається багатьма параметрами. В рекомендації МСЕ-T G.1028 наведені параметри оцінки якості, основні причини погіршення якості передачі мовного сигналу та алгоритм діагностики таких причин. Пошук методів усунення та мінімізації впливу факторів погіршення якості мовного сервісу в мережі LTE є актуальною задачею подальших досліджень.

Література

1. Технологія передачі голосу в мережі LTE, Ветошко Іван //[Електронний ресурс] – режим доступу: <http://conferenc.its.kpi.ua/2020>.
2. International Journal of Sciences: Basic and Applied Research “Design of Quality of Service Parameters for Voice over Long Term Evolution “LTE” Network”. Mohamed ELWakiela, Hesham ELBadawyb, Hadia Elhennawyc, 2016 (ISSN 2307-4531).
3. Ветошко І. П. Архітектура та технічні принципи функціонування ядра мережі мобільного зв'язку LTE: дипломна робота бакалавра телекомунікацій та радіотехніки: Київ, 2020, 73 с.
4. МСЭ-T G.1028: Качество обслуживания и технические характеристики мультимедийных систем – общие и связанные с пользователем аспекты //[Електронний ресурс] режим доступу: https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-G.1028.2-201906-I!!PDF-R&type=items.
5. GSM Association Official Document IR.42 - Definition of Quality of Service parameters and their computation Version 9.0 //[Електронний ресурс] – режим доступу: <https://www.gsma.com/newsroom/wp-content/uploads//IR.42-v9.0.pdf>.

ОСОБЛИВОСТІ РАДІОЧАСТОТНОЇ ФІЛЬТРАЦІЇ В SDR СИСТЕМАХ

Ільченко М.Ю., Кайденко М.М.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: kkk610@ukr.net

FEATURES OF RF FILTERING IN SDR SYSTEMS

This article presents the features of RF filtering in modern SDR systems. The relationship between the structure of building RF filters and the types of antenna systems used is shown. Variants of constructing RF filters for cognitive radio are proposed.

Програмно-визначувані радіосистеми (*Software-defined radio* - SDR) поєднують в собі передові технології для забезпечення гнучкості при створенні радіосистем. До цих технологій відносяться широкосмугові технології, радіочастотні компоненти, програмовані радіочастотні компоненти, технології цифрової обробки сигналів, аналогово-цифрові та цифро-аналогові перетворювачі, синтезатори частоти, технології побудови системи на кристалі, технології обробки інформації.

Стрімкий розвиток технології SDR пов'язаний в першу чергу з появою високоефективних, високоінтегрованих радіочастотних трансиверів, призначених для використання в системах зв'язку «точка-точка», фемто/піко/мікро базових станціях 3G та 4G і радіосистемах загального призначення, зокрема трансиверів, описаних в [1, 2].

Сучасні SDR трансивери мають в своєму складі інтегровані засоби фільтрації побічних каналів прийому приймачів та позасмугових випромінювань передавачів, які є програмованим і забезпечують більш ніж достатній рівень фільтрації. Однак, не зважаючи на наявність таких фільтрів, необхідність в використанні радіочастотних засобів фільтрації визначається в першу чергу наступними чинниками:

- вплив потужного сигналу передавача на вхід приймача в режимі частотного дуплексу (FDD) потребує встановлення фільтру-дуплексера (в режимі TDD він не потрібен);
- не залежно від режиму дуплексу на вхід приймача може діяти потужна завада від близько розташованих радіозасобів, потужність якої на вході може перевищувати допустимий рівень, що може призвести до введення приймача в режим нелінійного насичення.

Використання радіочастотних засобів фільтрації і їх характеристики визначаються призначенням SDR системи. Для систем, які працюють у відповідності до стандартизованих протоколів зв'язку (GSM, CDMA, WCDMA, 4G LTE, WiFi) можуть бути використані стандартні діапазонні радіочастотні фільтри, розроблені для використання в таких системах. У випадку використання SDR трансиверів для побудови когнітивного радіо для цих систем також не виникає особливих проблем при використанні,

оскільки в таких системах найчастіше використовуються “кратні” діапазони частот, або діапазони близькі до кратних, що може дозволити використовувати властивості мікросмужкових фільтрів СВЧ, наприклад на основі чвертьхвильових резонаторів з розподіленими параметрами, які мають “паразитні” смуги пропускання на частотах, що кратні основній гармоніці [3].

У випадку конгнітивного радіо, орієнтованого на використання широких смуг частот, можливості якого закладені в сучасних SDR трансиверах, виникає необхідність в використанні широкосмужкових фільтрів, або фільтрів зі змінною смугою пропускання в широкому діапазоні частот (змінною центральною частотою смуги пропускання). Розробці мікросмужкових фільтрів, в тому числі і з релюльованими параметрами автори приділяють велику увагу, що відображено наприклад в роботах [4, 5]. Найкращим варіантом перекриття широкої смуги частот SDR системою є комбінація побудови SDR трансивера та широкосмужкових фільтрів з використанням багатоканальних перепрограмованих вхідного тракту приймача та вихідного тракту передавача.

Побудова радіочастотної фільтрації SDR системи напряму залежить від того, яким чином будується антенна система. В документах та рекомендаціях SDR форуму цьому напрямку присвячується особлива увага, зокрема в роботі [6] визначається таксономія (систематика) відносно структури побудови антенних систем базових станцій, побудованих на базі SDR. Вона може бути поширена і на інші безпроводові системи, в яких використовується робота в більш ніж одному діапазоні частот та технологія SDR. На рис. 1 показано таку систематику і її типи.

Виділяються чотири типи антенних систем. Найпростішим є тип I, в якому використовується одиночна антена, при цьому система фільтрації буде традиційною.

Типи II та III відносяться до використання масивів антенних систем, при цьому тип II передбачає вибір антенної системи з формуванням діаграми спрямованості безпосередньо на радіочастоті (радіочастотна обробка). При цьому передбачається використання антенних систем з фіксованими, комутованими та скануючими діаграмами спрямованості.

На відміну від типу II в типі III діаграма приймальна діаграма спрямованості формується шляхом цифрової обробки в основній смузі частот. Перевага полягає в тому, що може бути сформована практично люба кількість приймальних пучків, які можуть скануватись індивідуально і не повинні бути ортогональними. Однак для передачі діаграма спрямованості повинна формуватись на радіочастоті, або на проміжній частоті таким же чином, як і для типу II. Характеристики передавальної діаграми спрямованості можуть бути оптимізовані на основі інформації, отриманої в результаті цифрової обробки на прийомі в основній смузі частот. Цей тип має властивість бути повністю адаптованим для прийому та високо адаптованим для передачі.

Тип IV передбачає комбінування та вибір (MIMO системи). При цьому часове, просторове, частотне та поляризаційне рознесення використовується

в системній обробці в основній смузі частот для покращення якості прийнятого сигналу. Може застосовуватись до любого з типів антенних систем. Застосовується при прийомі в основній смузі частот та використовується для мінімізації ефектів замирань внаслідок багатопроменевості. Алгоритми обробки в приймачі використовуються для визначення оптимальних налаштувань антенної системи передавача.

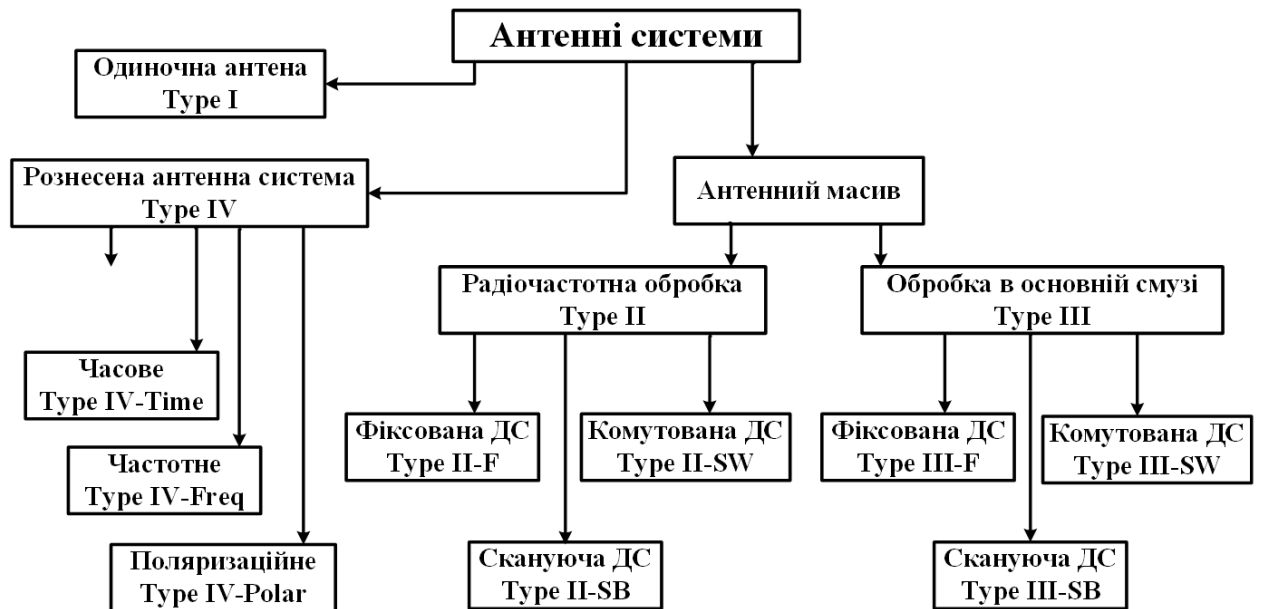


Рис.1. Систематика типів антенних систем програмно-визначуваних радіосистем.

Відповідно до типу використаного при побудові антенної системи, смуги робочих частот та кількості діапазонів застосовуються різні схеми побудови системи фільтрації, в основі якої лежать окремі радіочастотні фільтри, об'єднані в єдину систему радіочастотної фільтрації з фіксованими параметрами, комутованими або програмно переналаштовуваними.

Література

1. RF Agile Transceiver. AD9361. Data Sheet. - Режим доступу: <https://www.analog.com/media/en/technical-documentation/data-sheets/AD9361.pdf>
2. Integrated, Dual RF Transceiver. AD9371. Data Sheet. Режим доступу: <https://www.analog.com/media/en/technical-documentation/data-sheets/AD9371.pdf>
3. Маттей Д.Л., Янг Л., Джонс Е.М.Т. Фильтры СВЧ, согласующие цепи и цепи связи: В 2-х т. / Пер. с англ. под ред. Л.В. Алексеева и Ф.В. Кушнира. - М.: Связь, 1972, - 1 т. 222 с., - 2 т. 249 с.
4. A.V. Zakharov, M.Ye. Ilchenko Varicap-tuned narrowband filters with extended rejection band based on U-shaped microstrip resonators. Radioelectronics and Communications Systems. 2017. Vol. 60, No. 9, pp. 383-392. DOI: 10.3103/S0735272717090011.
5. A. Zakharov, S. Rozenko, and M. Ilchenko, "Varactor-Tuned Microstrip Bandpass Filter with Loop Hairpin and Compline Resonators," IEEE Trans. Circuits Syst. II, Exp. Briefs. Published 1.10.2018. DOI: 10.1109/TCSII.2018.2873227.
6. Software Defined Radio Forum. Base Station Working Group. Base Station System Structure. Document No. SDRF-01-P-0006-V2.0.0 — Режим доступу: http://www.sdrforum.org/pages/documentLibrary/documents/SDRF-01-P-0006-V2_0_0_BaseStation_Systems.pdf

АНАЛІЗ МОДЕЛЕЙ ВТРАТ НА ПОШИРЕННЯ ДЛЯ РАДІОЛІНІЙ ЗЕМЛЯ-ПОВІТРЯ

Кравчук С.О., Кравчук І.М.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail:sakravchuk@ukr.net

ANALYSIS OF PROPAGATION LOSS MODELS FOR GROUND-TO-AIR RADIO LINKS

This paper solves the problem of analytical selection of a fairly simple model for calculating signal propagation losses to support radio links from ground terminal to air platforms. The proposed approach to channel modeling is to separately consider the components of direct LOS (line of sight) and indirect NLOS visibility together with the possibilities of their occurrence.

На даний час розроблено багато різних моделей для оцінювання втрат щодо поширення радіосигналу на лінії "повітря-земля". Усі ці моделі призначені для вирішення певних вузьких задач, розв'язання яких дозволяє реалізувати зовсім різні за призначенням сценарії роботи радіообладнання на трасі "повітря-земля" (службові радіолінії управління авіонікою, моніторинг, навігація, радіолінії передачі даних, міжплатформенний зв'язок та ін.) [1, 2]. В даній роботі вирішується задача аналітичного вибору достатньо простої моделі розрахунку втрат на поширення сигналу для підтримки радіоліній наземний термінал-аероплатформа (висот до 1000 м), та її аналіз.

Пропонований підхід до моделювання каналу поширення "повітря-земля" полягає в тому, щоб окремо розглядати компоненти прямої LOS (line of sight) і непрямої NLOS видимості разом з можливостями їх виникнення. Зауважимо, що для випадку NLOS через ефект затінення і відображення сигналів від перешкод втрати на трасі вище, ніж LOS. Отже, на додаток до втрат при поширенні у вільному просторі, для ліній LOS і NLOS призначаються різні значення додаткових втрат на радіолінії (рис. 1). Таким чином в загальному вигляді середні втрати на радіотрасі "повітря-земля" можна записати у вигляді наступної функції: $\gamma_{av} = f(\gamma_0, p_{LOS}, \xi)$, де γ_0 - втрати на поширення у вільному просторі; p_{LOS} - ймовірність наявності радіотраси з прямою видимістю LOS при куті піднесення θ ; ξ - середні додаткові втрати (до втрат у вільному просторі) при поширенні, які залежать від навколишнього середовища.

Для вільного простору втрати на поширення радіохвиль, як добре відомо, будуть $\gamma_0 = 20 \lg(4\pi f_c d / c_0)$, дБ, де f_c – несуча частота, Гц; c_0 – швидкість світла; $d = (R^2 + h^2)^{1/2}$ – відстань між аероплатформою і наземним терміналом; R – наземна відстань між аероплатформою і наземним терміналом; h – висота зависання аероплатформи.

Ймовірність наявності радіотраси з прямою видимістю згідно [3] можна визначити із наступного рівняння $p_{LOS} = 1 / (1 + \alpha \times \exp(-\beta \times (180 / \pi \theta - \alpha)))$, де α і β - постійні значення, які залежать від навколишнього середовища (сільська, міська, щільна міська і т. д.). Наприклад для міста можна прийняти

$$\alpha = 9,6 \text{ і } \beta = 0,28.$$

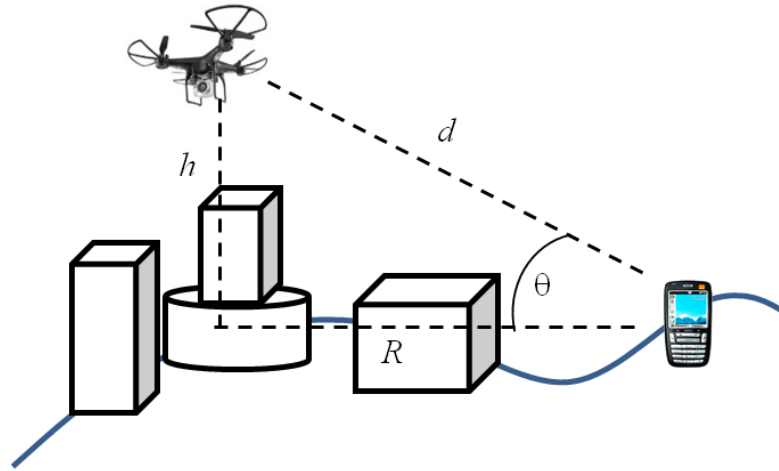


Рис. 1. Сценарій радіолінії аероплатформа-наземний термінал.

Тоді втрати на поширення радіохвиль в умовах прямої видимості можна записати як $\gamma_{\text{LOS}} = p_{\text{LOS}} (\gamma_0 + \xi_{\text{LOS}})$, а в умовах непрямої видимості - $\gamma_{\text{NLOS}} = (1-p_{\text{LOS}})(\gamma_0 + \xi_{\text{NLOS}})$. Величини ξ_{LOS} і ξ_{NLOS} мають досить різні значення. Так ξ_{LOS} приймає одиниці дБ і головним чином враховує незначне затінення на трасі LOS, а ξ_{NLOS} становить десятки дБ і враховує наявність навколишніх будівель, елементів рельєфу та рослинних затінь. Виходячи із виразів, наведених в роботі [4], можна записати наступне рівняння для $\xi_{\text{NLOS}} = 20 \lg(2 \sin(2\pi h_t h_r / \lambda / d))$, де λ - довжина хвилі; h_t і h_r - висота розташування передавача і приймача, відповідно; d - відстань між передавачем і приймачем.

Виходячи із вище зазначеного можна записати наступний вираз $\gamma_{\text{av}} = f(\gamma_0, p_{\text{LOS}}, \xi) = \gamma_{\text{LOS}} + \gamma_{\text{NLOS}}$.

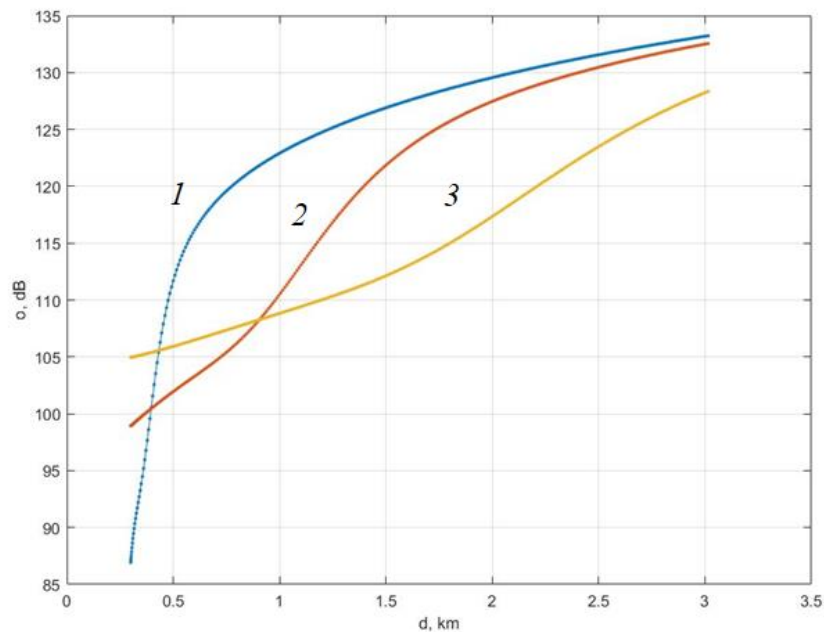


Рис. 1(а) Залежність втрат на поширення радіохвиль (графіки з Матлаб) від відстані між наземним терміналом і аероплатформою при різних величинах зависання останньої: 1 - 100, 2 - 400 і 3 - 800 м (a - з урахуванням втрат в умовах непрямої видимості).

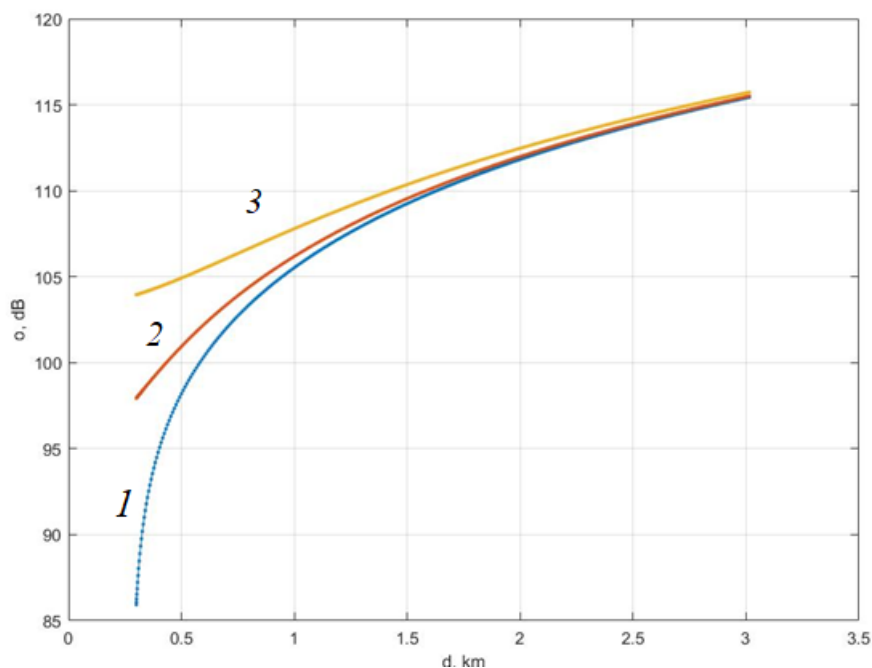


Рис. 1(б) Залежність втрат на поширення радіохвиль (графіки з Матлаб) від відстані між наземним терміналом і аероплатформою при різних величинах зависання останньої: 1 - 100, 2 - 400 і 3 - 800 м (β – без врахування втрат в умовах непрямої видимості).

Результати моделювання в пакеті Матлаб представлені на рис. 2 у вигляді залежностей втрат на поширення радіохвиль від відстані між наземним терміналом і аероплатформою при різних величинах зависання останньої. Як видно із рис. 2(б) в умовах прямої видимості втрати на поширення радіосигналу зростають зі збільшенням відстані між передавачем і приймачем, причому чим вище знаходиться аероплатформа, тим більші втрати на поширення. Однак видно, що при малих співвідношеннях наземної відстані і висоти зависання, тобто високих кутах місця θ , втрати а поширення сигналу будуть найменші. На рис. 2(а) представлено залежності із урахуванням втрат в умовах непрямої видимості, з яких видно, що чим вище аероплатформа знаходиться над землею (при наземних відстанях порядку величин зависання аеропалформи, що є типовим сценарієм для умов урбанізованого місця), тим менше значення втрат. Бо збільшується значення кута місця i , таким чином, зростає ймовірність LOS.

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).
3. Y. Zheng, Y. Wang, and F. Meng, "Modeling and simulation of pathloss and fading for air-ground link of HAPs within a network simulator," in Proc. of IEEE International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Beijing, China, Oct. 2013.
4. Y. S. Meng and Y. H. Lee, "Measurements and Characterizations of Air-to-ground Channel over Sea Surface at C-band with Low Airborne Altitudes," IEEE Transactions on Vehicular Technology, vol. 60, no. 4, pp. 1943–1948, (2011).

АПРОКСИМАЦІЯ ДІАГРАМИ СПРЯМОВАНOSTІ АНТЕНИ БАЗОВОЇ СТАНЦІЇ

Кравчук С.О., Рисцова К.І.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: sakravchuk@ukr.net

BASE STATION ANTENNA PATTERN APPROXIMATION

In this paper, a new approximation of the BS directional pattern in the horizontal and vertical planes is developed, the axes of which are interconnected by the geometry of the ellipse. Moreover, the plane of such an ellipse corresponds to the cross-sectional plane of the BS directional pattern with the position of the drone, which forms a radio channel with the BS and the user terminal.

На даний час мають місце багато різних моделей апроксимації секторних антен базових станцій (БС) систем мобільного зв'язку [1-3]. Однак кожна із відомих апроксимацій розроблена для певного сценарію з певними спрощеннями, які не можуть бути прийнятними для всіх можливих сценаріїв розгортання системи. Тому в даній роботі розроблено нову апроксимацію діаграми спрямованості БС в горизонтальній і вертикальній площинах, вісі яких пов'язані між собою геометрією еліпса. Причому площина такого еліпса відповідає площині перетину діаграми спрямованості БС з положенням дрону, який формує радіоканал із БС і користувацьким терміналом.

Потрібно провести оцінку положення дрона і користувацького терміналу UE по відношенню до обсягу діаграми спрямованості антени БС. Це важливо, тому що реалізація нашого сценарію можлива тільки в разі потрапляння дрона в опромінення антеною системи БС. Область діаграми спрямованості представимо у вигляді прямого конуса з вершиною в точці антеною системи БС, кутом розкриття $2\theta_{bs}$, який дорівнює ширині її головного променя на рівні 0,5 від її максимального значення за потужністю, і лінією висоти конуса, що збігається з головною віссю симетрії діаграми спрямованості антени БС. Площа трикутника (BS, O_2 , O_3), обертанням якого навколо головної осі діаграми спрямованості формується конус випромінювання БС, є площиною аналізу положення дрона в промені випромінювання антени БС. Визначимо ординати точки O_1 як точки найменшого відстані від дрона до головної осі симетрії антени БС. Виходячи з того, що точкою джерела випромінювання служить антена БС, то відстані до UAV і O_1 приймаємо рівними (однаковий радіус фронту хвилі від БС), тобто є $\rho = |BS, UAV| = |BS, O_1| = d_{bs-dr}$. Тоді координати точки O_1 (x_{o1} , y_{o1} , z_{o1}) можна визначити як $y_{o1} = \rho_x \sin \psi_{xy}$, $x_{o1} = \rho_x \cos \psi_{xy}$, $z_{o1} = z_{bs} - \rho \sin \psi_z$, де $\rho_x = \rho \cos \psi_z$ - проекція вектора ρ на площину (x , y).

Відстань між UAV і O_1 буде $d_{dr-o1} = [(x_{o1} - x_{dr})^2 + (y_{o1} - y_{dr})^2 + (z_{o1} - z_{dr})^2]^{1/2} = [(x_{o1} - l_{dr} \cos \phi_{xy})^2 + (y_{o1} - l_{dr} \sin \phi_{xy})^2 + (z_{o1} - h_{dr})^2]^{1/2}$.

Діаграма спрямованості антенної системи БС є секторною з різними розподілами електромагнітного поля у вертикальній і горизонтальній площині. Звідси в горизонтальній площині розкрив основного променя діаграми спрямованості, головним чином, має 60° , а у вертикальній - до 10° . Для простоти аналізу сценарію, який розглядається, скористаємося існуючими апроксимаціями діаграм спрямованості антен. Так у вертикальній площині скористаємося апроксимацією для вузько направленої діаграми згідно [4, 5]:

$$G_v(\varphi) = G_{\max} \sin^2(\pi n \varphi) / (n \sin^2(\pi \varphi)),$$

де n - ціле число, яке визначає крутизну спаду спрямованості головного пелюстка антени; φ - кут відхилення від електричної осі (головного пелюстка) антени; $G_{\max}$ - максимальне значення коефіцієнта підсилення головного пелюстка антени. Для апроксимації горизонтальної спрямованості характеристики головного пелюстка антени скористаємося виразом з [6]:

$$G_v(\varphi) = G_{\max} (\cos \varphi)^n.$$

Оскільки даний вираз не відтворює структуру бічних пелюстків, можна використовувати для моделювання плоске уявлення бічної пелюстки (воно зазвичай вказується виробником антен) наступним чином:

$$G_h(\varphi) = \max [G_{\max} (\cos \varphi)^n, G_0],$$

де G_0 - рівень перших бічних пелюстків діаграми спрямованості.

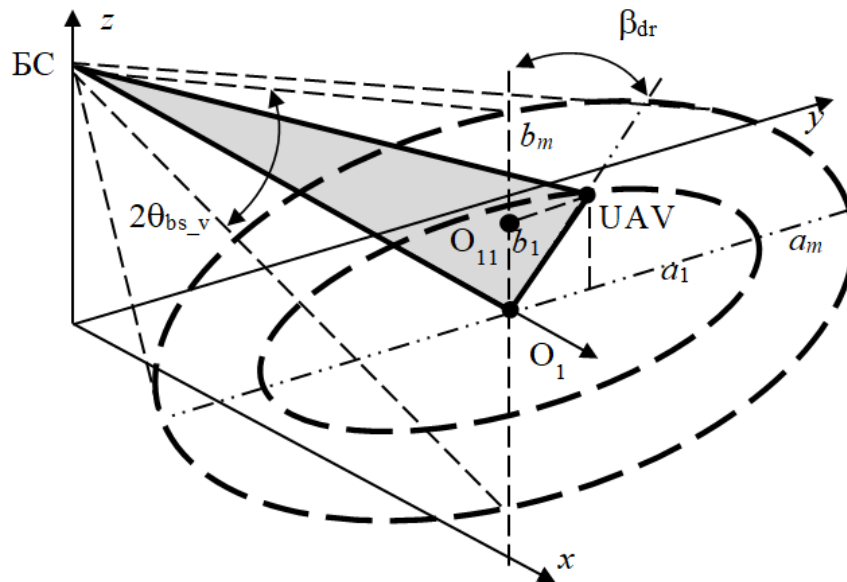


Рис. 1. Сценарій перетину діаграми спрямованості антени БС з еліптичною площиною, де розташований дрон (UAV – точка зависання дрону).

Перед нами стоїть завдання визначення положення дрона по відношенню до площини перетину діаграми спрямованості з метою визначення коефіцієнта підсилення в даній точці зависання дрона. Беручи еліптичний перетин діаграми спрямованості, отримуємо, що велику і малу осі еліпса перетину визначають кутові величини $2\theta_{bs\_v}$ і $2\theta_{bs\_h}$, відповідно. Тоді можна

визначити положення антени дрона як точку на дузі еліпса перетину. Для цього знаходимо кут β_{dr} відхилення положення антени дрона щодо вертикальної площини діаграми спрямованості в розглянутому еліптичному перетині. Визначаємо координати точки

$O_{11}(x_{o11}, 0, z_{dr})$ як проекції точки UAV на перпендикуляр до площини (x, y) , який проходить через точку O_1 , і відстань між UAV і O_{11} :

$$d_{dr-o11} = [(x_{o11} - x_{dr})^2 + (y_{o11} - y_{dr})^2 + (z_{o11} - z_{dr})^2]^{1/2} = [(x_{o11} - x_{dr})^2 + (y_{dr})^2]^{1/2},$$

а відстань між точками O_1 і O_{11} буде

$$d_{o1-o11} = [(x_{o11} - x_{o1})^2 + (y_{o11} - y_{o1})^2 + (z_{o11} - z_{o1})^2]^{1/2} = |z_{o11} - z_{o1}|.$$

Тоді кут відхилення можна визначити із $\beta_{dr} = \arcsin(d_{dr-o11}/d_{dr-o1})$.

Геометрію еліпса визначаємо: велика напіввісь a , лінія якої паралельна вісі $(0, y)$, і мала напіввісь b , лінія якої співпадає з перпендикуляром до площини

(x, y) і проходить через точку O_1 . Для еліптичного перерізу діаграми спрямованості антени БС на відстані $d_{bs-o1} = [(x_{o1})^2 + (y_{o1})^2 + (z_{o1} - z_{bs})^2]^{1/2}$ і при кутах розкриття $2\theta_{bs\_v}$ і $2\theta_{bs\_h}$ маємо розмір великої і малої напіввісей $2a_m = d_{bs-o1}/(2 \cos(4\theta_{bs\_h}))$ і $2b_m = d_{bs-o1}/(2 \cos(4\theta_{bs\_v}))$, відповідно. Звідси можна визначити співвідношення між півосями як

$$k_m = a_m/b_m = d_{bs-o1}/(2 \cos(4\theta_{bs\_h}))/d_{bs-o1}/(2 \cos(4\theta_{bs\_v})) = \cos(4\theta_{bs\_v})/\cos(4\theta_{bs\_h}).$$

Для всіх еліпсів, які можуть бути сформовані з центром в точці O_1 і всередині площі еліпса з a_m і b_m , матимуть $k_m = \text{const}$. Це дозволяє визначити еліпс перетину діаграми спрямованості (з півосями a_1 і b_1), на якому розташовується точка антени дрона UAV. Приведемо тривимірні координати UAV до двовимірних (x_{dre}, y_{dre}) на площині, яка утворюється еліпсами з початком координат в точці O_1 . Тут $x_{dre} = d_{dr-o11}$, $y_{dre} = d_{o1-o11}$. Тоді піввісь периметра еліпса, де розташований UAV, можна знайти як $a_1 = (y_{dre}^2 k_m^2 + x_{dre}^2)^{1/2}$, $b_1 = a_1/k_m$. Тепер можна визначити кути розкриття діаграми для еліптичного перетину з півосями a_1 і b_1 при допомозі співвідношень для рівнобедреного трикутника

$$2\theta_{1bs\_v} = \arccos(d_v/(4b_1)) \text{ і } 2\theta_{1bs\_h} = \arccos(d_h/(4a_1)),$$

де $d_v^2 = (d_{bs-o1})^2 - 4b_1^2$; $d_h^2 = (d_{bs-o1})^2 - 4a_1^2$; $d_{bs-o1} = [(x_{o1} - x_{bs})^2 + (y_{o1} - y_{bs})^2 + (z_{o1} - z_{bs})^2]^{1/2}$.

Визначивши необхідні робочі кути розкриття діаграми спрямованості антени БС, можна визначити значення коефіцієнта посилення в точках, які лежать на кінцях півосей еліпса, що проходить через антену дрона: $G_h(\theta_{1bs\_h})$ і $G_v(\theta_{1bs\_v})$. Тобто $G_{vy} = G_v y_1/b_1$; $G_{hx} = G_x x_1/a_1$; $x_1 = d_{dr-o1} \sin(\beta_{dr})$; $y_1 = d_{dr-o1} \cos(\beta_{dr})$; $G_{dr} = (G_{vy} G_{hx})^{1/2}$.

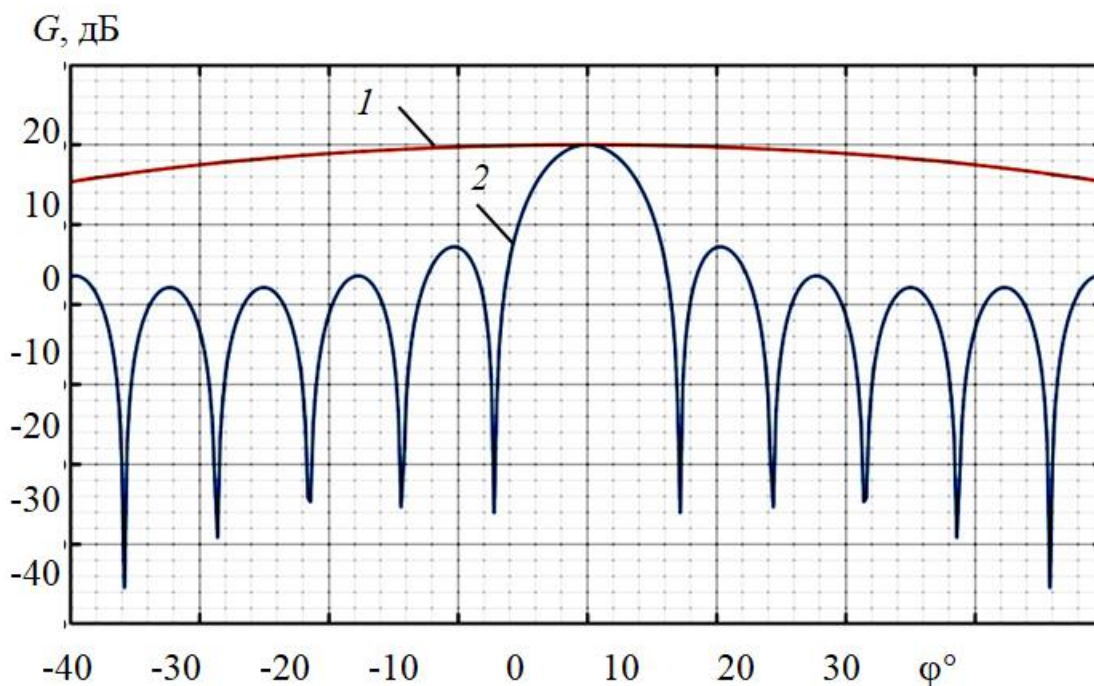


Рис. 2. Апроксимація діаграми спрямованості антени БС в площинах ($G_{\max} = 20$ dB):

1 - горизонтальний $2\theta_{bs\_h} = 60^\circ$ ($n = 4$);

2 - вертикальний $2\theta_{bs\_v} = 6,4^\circ$ ($n = 8$)

Результати моделювання на базі запропонованої моделі апроксимації діаграми спрямованості в пакеті Матлаб представлено на рис. 2.

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).
3. Kaidenko M., Kravchuk S. Autonomous Unmanned Aerial Vehicles Communications on the Base of Software-Defined Radio. In: Ilchenko M., Uryvsky L., Globa L. (eds) Advances in Information and Communication Technology and Systems. MCT 2019. Lecture Notes in Networks and Systems, vol 152. Springer, Cham. pp. 289-302 (2019) https://doi.org/10.1007/978-3-030-58359-0_16.
4. N. Deng, M. Haenggi, “A Novel Approximate Antenna Pattern for Directional Antenna Arrays”, IEEE Wireless Communications Letters, Vol. 7, Issue 5, pp. 832 – 835 (2018) (DOI: 10.1109/LWC.2018.2829741).
5. X. Yu, J. Zhang, M. Haenggi, and K. B. Letaief, “Coverage analysis for millimeter wave networks: The impact of directional antenna arrays,” IEEE Journal on Selected Areas in Communications, vol. 35, no. 7, pp. 1498–1512, Jul. 2017 (DOI: 10.1109/JSAC.2017.2699098).
6. Balanis C.A. Antenna theory: Analysis and design. - N.Y.: John Wiley & Sons, 1996. - 960 p.

ЗАГРОЗИ БЕЗПЕЦІ ТА ПРОБЛЕМИ ВРАЗЛИВОСТІ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Гетьман О.В., Кайдено М.М., Роскошний Д.В.

Інститут телекомунікаційних систем КІП ім. Ігоря Сікорського, Україна

E-mail: kkk610@ukr.net

SECURITY THREATS AND UAV VULNERABILITY ISSUES

The article discusses the vulnerabilities of unmanned aerial vehicles. The classification of attacks for various features is given. The taxonomy of various types of known attacks, which can be exposed to UAVs, is presented.

Сьогодні безпілотні літальні апарати (БПЛА) використовуються в різних областях, таких як моніторинг, пошуково-рятувальні місії, комерційні послуги, наукові дослідження, сільське господарство, а також у військових цілях. БПЛА корисні в різних областях, але безпека завжди була головною проблемою. Крім того, БПЛА несе конфіденційну інформацію, пов'язану з конфіденційністю людей, і викликає серйозні проблеми, якщо дані використовуються зловмисниками. Було багато спроб вирішити проблеми безпеки БПЛА, але немає типового способу захистити БПЛА від різноманітних атак.

Важливим аспектом атак на БПЛА, включаючи його викрадення, який слід підкреслити, - це цілеспрямована атака, в тому числі і кібератака з точки зору термінології кібервійни [1], яка охоплює експлуатацію, напад, захист і асиметричну відповідь в цілому. Спроба викрадення - це комбінація кібер і електронних операцій/зусиль, а не захоплення одним клацанням миші, оскільки для цього потрібно кілька інструментів і різних методів з областей кібернетичної війни і електронної війни одночасно в серії дій для досягнення своєї мети, особливо коли метою є несанкціоноване використання безпілота в терористичних цілях, або коли це є військовий БПЛА. Багатоступінчастий характер сучасних атак на БПЛА, заснований на координації індивідуальних дій [2], включає повністю виконану атаку з захопленням БПЛА, або перехопленням інформації. При цьому важливо знати всі вразливості безпілотного апарату та можливі дії зловмисників при атаках на нього.

Основними жертвами порушення безпеки безпілотного апарату є різні компоненти системи, такі як пристрої, мережі та канали зв'язку [3]. При цьому класифікація атак може здійснюватися за різними ознаками.

Всі атаки на БПЛА за місцем нанесення умовно можна розділити на:

- атаки, які здійснюються безпосередньо на БПЛА через безпроводові канал зв'язку, управління та телеметрії;
- атаки, які здійснюються на мережу управління БПЛА;
- атаки, які здійснюються на програмне забезпечення БПЛА.

Атаки на БПЛА за часом здійснення діляться на:

- атаки в реальному масштабі часу;
- атаки з відкладеним часом.

Атаки на БПЛА за цілями нанесення можна розділити на:

- атаки спрямовані на фізичне знищення БПЛА;
- атаки спрямовані на перехоплення управління БПЛА з метою несанкціонованого використання, або викрадення;
- атаки спрямовані на перехоплення інформації про БПЛА та цільової інформації, для отримання якої використовується безпілотний апарат, наприклад відео, дані з датчиків.

Типи атак, які застосовуються зловмисником істотно можуть відрізнятися в залежності від цільового використання БПЛА та способу його управління:

- автономний БПЛА з ручним управлінням оператором з автономного пульта;
- автономний БПЛА з автоматичним управлінням польотом за завданням з автономного пульта;
- автономний БПЛА з мережевим управлінням з використанням безпроводових технологій та мереж;
- мережа БПЛА (рій дронів) з автоматичним управлінням польотом, включаючи мережеве управління.

Загрози безпілотному апарату та корисній інформації, для збору та обробки якої він застосовується, несуть відповідальність за порушення безпеки і призводять до великих втрат з точки зору ресурсів, довіри і доступності [4]. На основі цих вразливостей атаки та їх вплив можна розділити на п'ять основних типів. На рис.1 представлена таксономія різних типів відомих атак на безпілотні апарати, які можуть бути застосовані в залежності від цільового використання апарату, його типу та класу і цілей атаки.

Секретність є важливою проблемою для орієнтованої на дані безпеки, які збираються та обробляються за допомогою БПЛА, а обробка даних збільшує можливості загроз та вразливостей. Зловмисник націлений на безпілотний апарат для отримання конфіденційної інформації за допомогою різних підходів.

Цілісність визначає, що дані, які отримуються за допомогою БПЛА повинні бути послідовними, точними та надійними. Нелегітимні користувачі, або зловмисники не повинні змінювати передані дані в процесі обміну ними. Деякі з часто використовуваних механізмів захисту цілісності даних - це хеш-функції, контрольні суми тощо.

Конфіденційність гарантує, що інформація не може передаватися нелегітимним користувачам та бути отримана зловмисниками. Багато атак на БПЛА та наземну станцію управління є наслідком недоліків у безпеці. На конфіденційність впливає нелегітимний доступ для отримання корисної інформації.

Доступність визначається як послуги, що ініціюються негайно, коли це необхідно для підтримання правильної роботи. Доступність інформації полягає в тому, щоб законний користувач безпілотного апарату може

отримати доступ до інформації на основі своїх вимог. БПЛА використовуються областях, які орієнтовані на виконання конкретних задач, тому доступність є основною проблемою щодо безпеки.

З новим етапом розвитку технологій пов'язані нові ризики. **Довіра** є важливим активом, і на неї впливають багато вимірюваних та невимірних властивостей, таких як , міцність, надійність, доступність та здатність. Безпека та конфіденційність - це дві, категорії, які впливають на довіру. Довірчі відносини залежать від організацій, які займаються розробкою та експлуатацією БПЛА. Різні загрози довірі виникають через неправильну конфігурацію та обмежене включення механізмів безпеки на етапах розробки та розгортання.

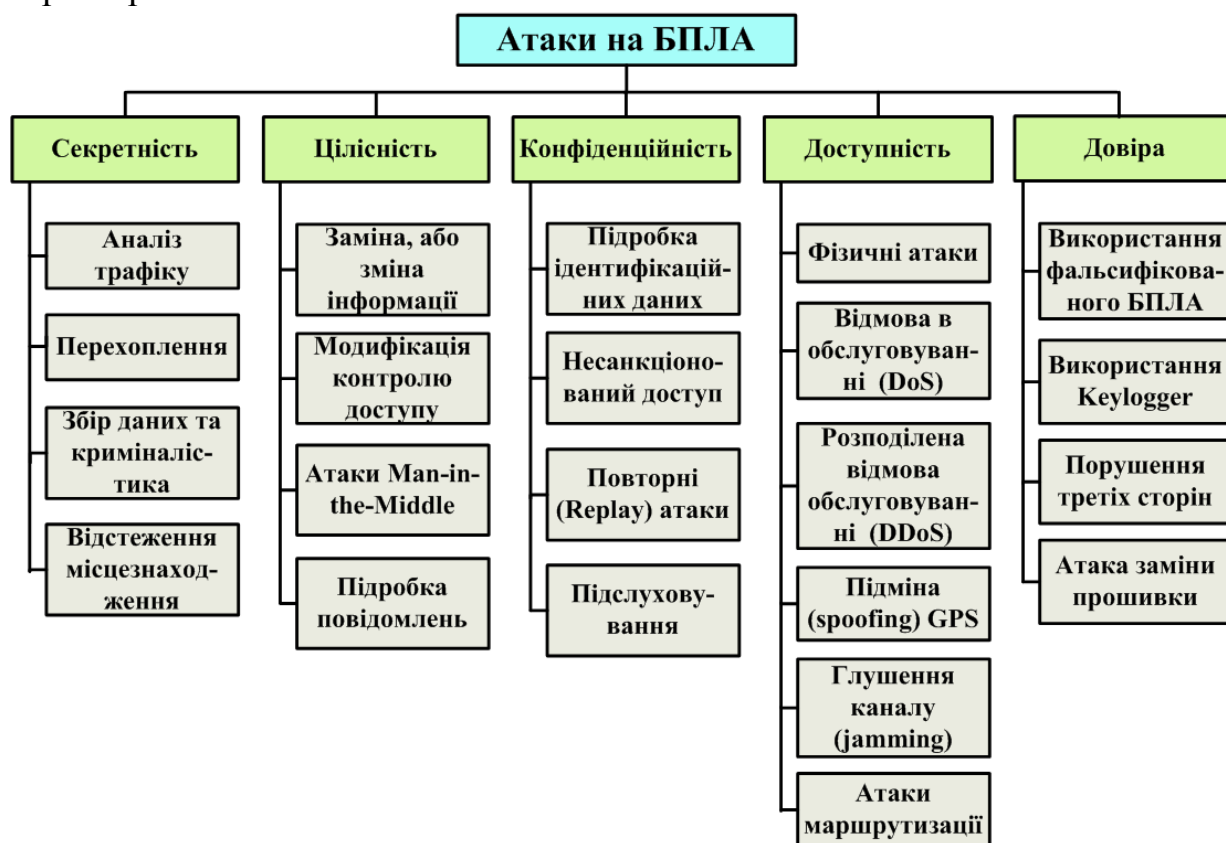


Рис.1. Таксономія різних типів відомих атак на БПЛА.

Література

1. S. M. Giray, "Anatomy of unmanned aerial vehicle hijacking with signal spoofing," *2013 6th International Conference on Recent Advances in Space Technologies (RAST)*, Istanbul, Turkey, 2013, pp. 795-800, doi: 10.1109/RAST.2013.6581320.
2. Yaacoub JP, Noura H, Salman O, Chehab A. Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet of Things*. 2020;11:100218. doi:10.1016/j.iot.2020.100218
3. M. Yampolskiy, P. Horvath, X. D. Koutsoukos, Y. Xue, and J. Sztipanovits. Taxonomy for description of cross-domain attacks on cps. In *Proc. of the 2nd ACM international conference on High confidence networked systems*, Philadelphia, Pennsylvania, USA, pages 135–142. ACM, April 2013.
4. K. Mansfield, T. Eveleigh, T. H. Holzer, and S. Sarkani. Unmanned aerial vehicle smart device ground control station cyber security threat model. In *Proc. of the IEEE Conference on Technologies for Homeland Security (HST'12)*, Waltham, MA, USA, November.

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ SYSTEM-ON-CHIP INTEL ТА XILINX ПРИ РОЗРОБЦІ SDR СИСТЕМ

Кайденко М.М., Роскошний Д.В.
*Інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: kkk610@ukrl.net*

FEATURES OF USING SYSTEM-ON-CHIP INTEL AND XILINX IN THE DEVELOPMENT OF SDR SYSTEMS

The advantages and importance of the use of SOC technologies in the development of modern SDR systems are considered. The analysis of the software for development from the leading manufacturers is carried out. The problems that arise during the transition to a hardware platform of another manufacturer are considered.

Програмно визначені радіосистеми (SDR) - це системи радіозв'язку, де компоненти, які традиційно впроваджуються в апаратне забезпечення (наприклад, змішувачі, фільтри, підсилювачі, модулятори / демодулятори, детектори тощо), замість цього реалізуються за допомогою програмного забезпечення на персональному комп'ютері або за допомогою вбудованих систем, в яких обчислювальні елементи побудовані на сучасних пристроях обробки сигналів, таких як процесори загального призначення (GPP), цифрові сигнальні процесори (DSP), програмовані логічні інтегральні схеми (FPGA), системи-на-кристалі (SoC) та ін.

На теперішній час розробка і застосування систем-на-кристалі є одним з найбільш перспективних напрямків у розробці електронної техніки.

У загальному випадку SoC є подальшим розвитком технології FPGA і являють собою інтегровані в одному кристалі процесорне ядро (ядра), блок програмованої логічної матриці FPGA, а також апаратно або програмно реалізовані модулі управління периферійними пристроями [1].

Використання SoC в програмно визначених радіосистемах надає розробникам та користувачам ряд істотних переваг, а саме:

- можливість застосовувати різні методи модуляції з використанням одного загального набору апаратних засобів;
- можливість змінювати функціональність пристрою лише змінюючи програмне забезпечення;
- можливість адаптивного вибору режиму роботи пристрою, що найкраще відповідає поточним умовам його експлуатації.
- виключення зі складу пристрою аналогового обладнання та зменшення його вартості, що призводить до спрощення радіосистеми та покращення її характеристик;
- можливість проведення досліджень без розробки нової апаратної платформи.

На сьогоднішній день основними виробниками апаратно-програмних засобів для розробки SoC є компанії Altera та Xilinx, які з недавнього часу є підрозділами компаній Intel та AMD відповідно.

Обидва виробники в спектрі своєї продукції для задоволення різних потреб ринку мають декілька класів SoC - від пристроїв найвищої щільності та продуктивності до найбільш економічно вигідних:

- Сімейства Stratix та Zynq Ultrascale+ MPSoC (EV) - високопродуктивні, найсучасніші пристрої.
- Сімейства Arria та Zynq Ultrascale+ MPSoC (CG) забезпечують оптимальну продуктивність та енергоефективність.
- Сімейства Cyclone та Zynq-7000 розроблені для створення малопотужних та економічно важливих проектів [2,3].

Порівняння програмних засобів для створення проектів на основі SoC від обох виробників наведено в таблиці 1 [4,5].

Таблиця 1. Порівняння програмних засобів.

Xilinx	Intel	Опис
Vivado HL System Edition 1. UltraScale 2. UltraScale+ 3. 7 Series	Intel Quartus Prime Pro Edition Intel Stratix 10, Intel Arria 10, Intel Cyclone 10 GX	Оптимізовано для підтримки найсучасніших SoC.
	Intel Quartus Prime Standard Edition for: • Stratix V • Arria series • Cyclone V, Cyclone 10 LP	Оптимізовано для підтримки попередніх поколінь SoC
Vivado HL WebPACK Edition	Intel Quartus Prime Lite Edition	Безкоштовна версія ПЗ з обмеженою підтримкою кристалів та IP
SDAccel Environment Деякі UltraScale та 7 Series пристрої.	Intel FPGA SDK for OpenCL™ Intel Stratix 10, Intel Arria 10, Cyclone V SoC	Середа розробки для OpenCL
SDSoC Environment	Intel SoC FPGA Embedded Development Suite	Комплексний засіб розробки ПЗ для вбудованих систем
Software Development Kit	Nios® II Embedded Design Suite (EDS)	Комплексний засіб розробки та відлагодження ПЗ для SoC
System Generator for DSP	DSP Builder for Intel FPGAs	Засіб розробки для систем ЦОС
Vivado High-Level Synthesis	Intel HLS Compiler	Засіб розробки для High-Level synthesis

Отже, обидві компанії надають своїм користувачам широкий спектр функціонально схожих засобів для розробки своїх проектів. Але, традиційно, існують відмінності між цими засобами. Так, програмні засоби від Intel

мають більш сприятливий інтерфейс користувача та достатньо простий механізм створення та інтеграції апаратно-програмних блоків (IP core).

В той же час Xilinx відома якістю технічної підтримки користувачів, оскільки володіє більш широкою «базою знань» та найбільш повними рекомендаціями по застосуванню апаратно-програмних блоків в своїх пристроях.

Досить часто перед розробниками в силу різних обставин повстає завдання переходу на апаратну платформу іншого виробника. Зазвичай, більших зусиль потребує перехід з платформи Xilinx на платформу Intel. Кількість зусиль і час, необхідний для переходу, залежать від складності дизайну.

SoC-модулі містять в своєму складі блок системи обробки (PS) і блок програмованої логіки (PL). Ці два блоки повинні бути сконфігуровані та налаштовані на створення робочої системи, на якій запускається програмне забезпечення [6,7].

Конфігурація PS включає ідентифікацію периферійних пристроїв та налаштування окремих компонентів у системі. Визначення периферії для переходу відносно просто. Потрібно визначити периферійні пристрої, які є частиною поточного дизайну, а потім зіставити їх із тими, що підтримуються новою апаратною платформою.

Отже особливої уваги потребує визначення способу підключення периферії. Зазвичай використовуються порти між PS та PL (HPS та FPGA для Intel), які є подібними, але мають відмінності. Для Xilinx використовують порти AXI загального призначення, високопродуктивні AXI порти, порт ACP, тощо. Для Intel існує інтерфейс FPGA-to-SDRAM, FPGA-to-HPS bridge, HPS-to-FPGA bridge та lightweight HPS-to-FPGA Bridge.

Також слід звернути увагу на відмінності інтерфейсних сигналів (полярність, часові характеристики, тощо).

При перенесенні частини проекту, що має бути розташована в FPGA, синтезований код HDL, повинен бути сумісним із засобами проектування без змін.

Література

1. Kaidenko M.M., Roskoshnyi D.V. (2019) Software Defined Radio in Communications. 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 DOI https://doi.org/10.1007/978-3-030-16770-7_11 Print ISBN 978-3-030-16769-1.
2. <https://www.xilinx.com/products/silicon-devices/soc.html>.
3. <https://www.intel.ru/content/www/ru/ru/products/programmable/soc.html>.
4. https://www.xilinx.com/support/documentation/sw_manuals/xilinx2019_2/ug898-vivado-embedded-design.pdf.
5. https://www.intel.com/content/dam/www/programmable/us/en/pdfs/literature/ug/ug_soc_eds.pdf
6. https://www.xilinx.com/support/documentation/sw_manuals/ug1192-xilinx-design-for-intel.pdf.
7. <https://www.intel.com/content/dam/www/programmable/us/en/pdfs/literature/an/an307.pdf>.

ДОСЛІДЖЕННЯ ВИКОРИСТАННЯ АПАРАТНИХ ТЕХНОЛОГІЙ 60 ГГц СТАНДАРТУ IEEE 802.11AD ДЛЯ ЗАСТОСУВАННЯ В МІСЬКІЙ ЗАБУДОВІ

Кравчук С.О., Афанасьєва Л. О.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: liana.afanasyeva@gmail.com

EXPLORING THE POSSIBILITY OF USE HARDWARE TECHNOLOGY 60 GHZ THE IEEE 802.11AD FOR APPLICATIONS IN URBAN DEVELOPMENT

The development of the millimeter wave range is a promising direction for the development of high-speed mobile broadband radio access systems. The possibility of using 60 GHz hardware technologies of the IEEE 802.11ad standard, which is used indoors, for applications in urban development has been investigated.

Стрімке зростання використання мобільного широкосмугового доступу значно збільшує вимоги до пропускної здатності. Існуючі методи збільшення ємності досягли своїх меж: спектральна ефективність повільно наближається до межі Шеннона, а придбання більшої кількості спектра задовольняє лише обмежений приріст ємності та вимагає високих грошових витрат. Таким чином, щоб забезпечити збільшення пропускної здатності для мобільних додатків, необхідно розглянути нові підходи до доставки безпроводового контенту. [1-2]

Освоєння міліметрового діапазону хвиль є перспективним напрямком для розвитку високошвидкісних мобільних систем широкосмугового радіодоступу. Використання вузьконаправлених променів в міліметрових діапазонах хвиль дозволяє значно зменшити завади, які властиві цим частотам. Смуга 60 ГГц забезпечує 7 ГГц неліцензійного спектра для вимогливих до смуги пропускання мобільних додатків і підтримується стандартом IEEE 802.11ad (в даний час націлений на мультигігабітні безпроводові мережі всередині приміщень), який визначає кілька швидкостей передачі даних від 385 Мбіт/с до 6,76 Гбіт/с [3-5].

Дослідження проводились з використанням випробувального стенду з топологією «точка-точка», розгорнутого в міському середовищі (м. Київ) при наявності прямої видимості без перешкод (дерева і будівлі є серйозними перешкодами для нормальної роботи). Схема радіолінії, що досліджується представлено на рисунку 1. Канал WiGig IEEE 802.11ad складається з пари радіомодулів (безпроводових точок доступу), що можуть працювати в

режимах клієнтської контрольної точки (CP- control point) або точки доступу (AP- access point).

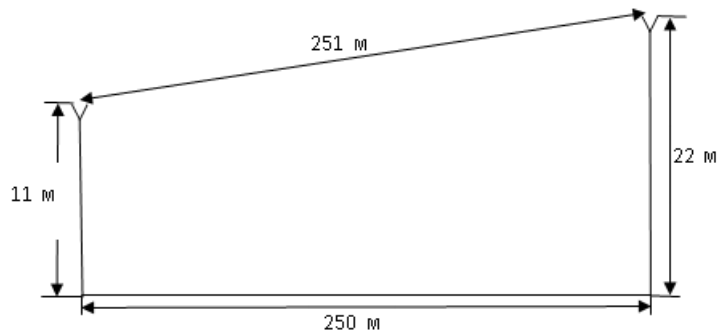
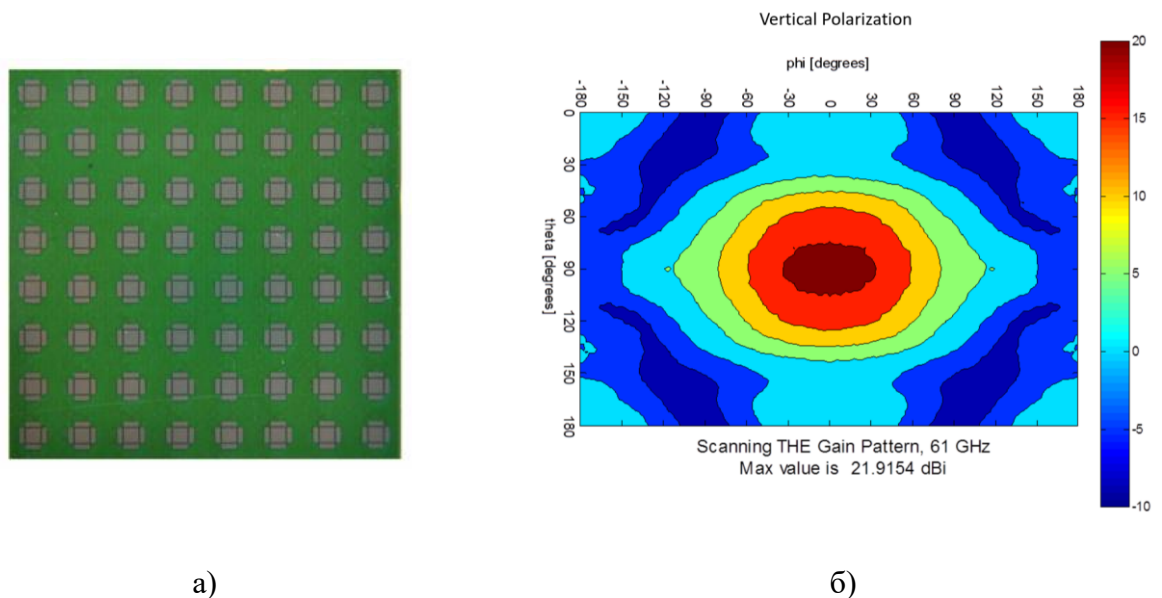


Рис. 1. Схема траси розповсюдження сигналу.

Для подолання загасання і зменшення перешкод радіолінії 60 ГГц використовувалася радіостанція на базі антенних решіток 8×8 для формування променя і концентрації енергії передачі в бажаному напрямку (рис.2). Радіоприймачі з антенними решітками здійснювали спрямовану передачу з використанням електронного керування променем, застосовуючи обробку сигналів в основній смузі частот для регулювання напрямків променя з мінімальною затримкою.



а)

б)

Рис. 2.- Характеристики радіомодуля 60 ГГц:
а) антенна фазована решітка з 64 патч-елементів;
б) діаграма спрямованості антени.

При проведенні досліджень було встановлено, що ефективна швидкість передачі даних під час сонячної погоди і при опадах (у вигляді дощу)

відповідає показникам близько 700 Мбіт/с при дальності зв'язку 250 м. Це підтверджує, що на відстанях порядку 100+ м радіолінія 60 ГГц досить стійка до погодних умов. Експериментально отримано, що в дощі інтенсивністю близько 3 мм/год втрати показника рівня сигналу RSSI приблизно 1,5 дБм, що не призводить до значного погіршення зв'язку. Таким чином, зроблено висновок, що точки доступу на базі антенних решіток розміром 8×8 можуть підтримувати діапазон відстаней 100+ м зі швидкістю 700 Мбіт/с навіть в умовах сильного дощу.

Стандарт IEEE 802.11ad для 60 ГГц визначає ряд схем модуляції і кодування для адаптації до різних швидкостей передачі. З огляду на необхідність адаптації до набагато більш динамічного зовнішнього середовища, ніж внутрішні мережі, для яких в даний час призначений стандарт 802.11ad, було визначено, що пропускна здатність UDP трафіку сягає значень близько 800 Мбіт/с з MCS4 і MCS6 для каналів 62640 МГц та 60480 МГц при RSSI -64 дБм і -65 дБм відповідно.

Виміри показали можливість застосування радіомодулів 60 ГГц стандарту IEEE 802.11ad в мережах 5G. Застосування радіомодулів з частотою 60 ГГц в якості пікосоти на вулицях, дозволять розширити можливості існуючих стільникових мереж і забезпечити збільшення пропускної здатності. Проте, радіолінія 60 ГГц може бути легко заблокована людським тілом враховуючи, що втрати становлять близько 20-50 дБ.

Література

1. Ільченко М.Ю., Кравчук С.О. Телекомунікаційні системи. – К.: Наукова думка, 2017.
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. M. Shafi, A. F. Molisch, P. J. Smith et al., “5G: A tutorial overview of standards, trials, challenges, deployment, and practice,” IEEE Journal on Selected Areas in Communications, vol. 35, no. 6, pp. 1201–1221, 2017.
4. Y. Niu, Y. Li, D. Jin, L. Su, and A. V. Vasilakos, “A survey of millimeter wave communications for 5G: Opportunities and challenges,” Wireless Netw., vol. 21, no. 8, pp. 2657–2676, Sep. 2014.
5. Kravchuk S., Afanasieva L. "Best" relay selection algorithm for wireless networks with cooperative relaying In: Proceedings of the 2019 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Odessa, Ukraine, 9–13 September 2019, pp. 1–4. IEEE Conference Publications (2019). 10.1109/UkrMiCo47782.2019.9165410. (IEEE Xplore Digital Library).

КООПЕРАТИВНА РЕТРАНСЛЯЦІЯ НА ОСНОВІ АДАПТИВНОГО ДЕКОДУВАННЯ

Урніш В. С., Кравчук С. О.

Інститут телекомунікаційних систем КІП ім. Ігоря Сікорського, Україна

E-mail: tmverauro@gmail.com

COOPERATIVE RELAY BASED ON ADAPTIVE DECODING

This paper will consider the adaptive decode-and-forward protocol. Options for constructing a simple and complex decode-and-forward protocol are considered. The purpose of this protocol is to minimize the reception of messages with errors.

Метою даної роботи є представлення адаптивного протоколу декодування та передачі. Розглядаються варіанти побудови простого та складного протоколу передачі. Які дозволяють мінімізувати отримання помилкових повідомлень.

На даний час спостерігається невпинне зростання трафіку передачі даних і вагома його частина, особливо в системах абонентського доступу, припадає на безпроводові системи. Усе більше користувацької інформації передається за допомогою безпроводових каналів, які знаходяться в одному частотному діапазоні. Збільшення навантаження на канали передачі підвищує рівень завад, що, у свою чергу, призводить до збільшення втрат поширення сигналу на радіотрасі. Підвищення завадостійкості каналу передачі зменшує вірогідність бітової помилки, що забезпечує безпосереднє підвищення якості прийнятого сигналу. Для цього доцільним рішенням є використання спеціальних протоколів та алгоритмів щодо забезпечення завадостійкої передачі даних [1-6], зокрема, протоколу простого адаптивного декодування та передачі.

Метою даної роботи є представлення адаптивного протоколу декодування та передачі. Розглядаються варіанти побудови простого та складного протоколу передачі. Які дозволяють мінімізувати отримання помилкових повідомлень.

В останній час з'явилася концепція так званої кооперативної ретрансляції. Вона дозволяє поєднати сигнали передачі від усіх ретрансляторів на цільовому приймачі, що підвищує просторове різноманіття радіорелейних систем. Принцип дії такої схеми можна представити таким чином: робоча радіолінія між двома бездротовими терміналами (джерело і цільової приймач), в якийсь момент часу погіршується настільки, що коефіцієнт бітових помилок переданих даних досягає свого гранично допустимого значення. При традиційній ретрансляційній системі для якісної передачі інформації від джерела до приймача формується обхідна радіолінія

через допоміжний термінал-ретранслятор. Але більшість схем кооперації страждають від таких недоліків, як потреба у каналі зворотного зв'язку, доступність інформації про стан каналу на передавачах, у порівнянні зі звичайною ретрансляцією збільшення загальної кількості передавальних вузлів або погіршення коефіцієнта бітових помилок та ін.

Мають місце два варіанти побудови адаптивного протоколу декодування-та-передачі: простий та складний.

Простий адаптивний протокол декодування-та-передачі (AdDF): джерело S надсилає інформацію безпосередньо і одночасно через ретранслятор R до цільового приймача D (рис. 1, а). Встановлення зв'язку відбувається у дві фази, що обумовлено нездатністю ретранслятора одночасно передавати та приймати на одній частоті.

В першій фазі джерело S передає свою інформацію. При цьому і ретранслятор, і цільовий приймач отримують однакові версії цього сигналу з шумом. Виходячи з аналізу якості прийнятого сигналу, ретранслятор приймає рішення чи проводити декодування-та-передачу, чи ні. Для сигналу достатньої енергетики він декодує і передає, у іншому випадку утримується від цього. Рішення може бути реалізоване, наприклад, шляхом циклічної перевірки на надмірність CRC (cyclic redundancy check) або за допомогою простого порогу відношення сигнал/шум SNR.

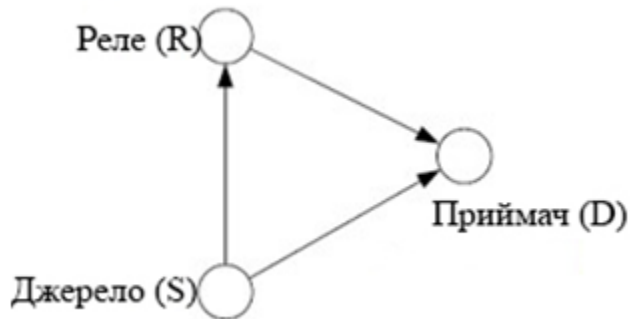


Рис. 1. Симетрична конфігурації безпроводової мережі із кооперативною ретрансляцією.

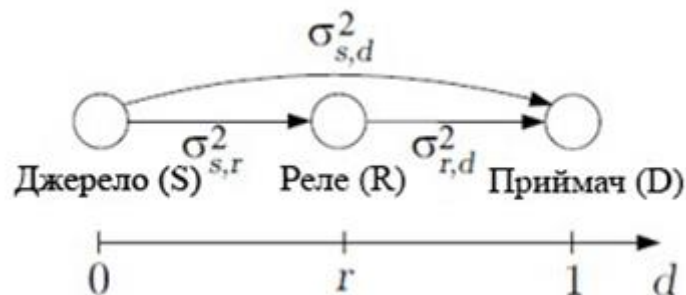


Рис. 2. Асиметрична конфігурація безпроводової мережі із кооперативною ретрансляцією.

На другій фазі, якщо ретранслятор вирішив передавати, він знову відправляє, прийнятий від джерела, сигнал до цільового приймача. Останній обробляє разом цю отриману версію сигналу із збереженими зразками посилянь, які він раніше отримав від джерела. В іншому випадку, тобто якщо ретранслятор вирішив не декодувати сигнал від джерела, то він не виконує передачі. Цільовий приймач виявляє цей випадок на основі відсутності достатньої потужності сигналу, і для демодуляції йому потрібно покладатися на зразки, збережені у фазі 1.

Такий протокол забезпечує досягнення просторового розмаїття, оскільки при хороших умовах каналу ретранслятор часто декодує та передає копії вихідної інформації по некорельованому каналу до цільового приймача. Одночасно отримується вигода від зменшення втрат на шляху: ретрансляційна станція, розташована між джерелом і цільовим приймачем, буде приймати повідомлення, що передаються джерелом, набагато надійніше, ніж цільовий приймач, і, в свою чергу, їй потрібно використовувати значно меншу потужність передачі, щоб "дістати" до цільового приймача.

Складний адаптивний протокол декодування-та-передачі (AdDF): такий протокол відрізняється від простого протоколу AdDF для того випадку, коли ретранслятор прийняв рішення не передавати повідомлення. Складний протокол запобігає виникненню "тиші", змушуючи джерело повторити своє повідомлення. Очевидно, що виграш від стандартного повторного кодування відбувається за рахунок підвищеної складності, оскільки джерело повинно мати інформацію про стан декодування ретранслятору.

Література

1. J. N. Laneman, D. N. C. Tse, and G. W. Wornell, Cooperative Diversity in Wireless Networks: Efficient Protocols and Outage Behavior, IEEE Trans. Inform. Theory, Apr. 2003, (accepted for publication).
2. M. Dohler, A. Gkelias, and H. Aghvami, 2-Hop Distributed MIMO Communication System, IEEE Electronics Letters, June 2003.
3. E. Zimmermann, P. Herhold, and G. Fettweis, On the Performance of Cooperative Diversity Protocols in Practical Wireless Systems, in Proc. 58th IEEE Vehic. Technol. Conf., Orlando, FL, Oct. 2003.
4. P. Herhold, A Simple Cooperative Extension to Wireless Relaying- Appendix, Feb. 2004.
5. S. M. Alamouti, A Simple Transmit Diversity Technique for Wireless Communications, IEEE J. Select. Areas Comm., vol. 16, no. 8, pp. 1451-1458, Oct. 1998.
6. John G. Proakis, Digital Communications, McGraw-Hill International Editions, 4th edition, 2002.

ОСОБЛИВОСТІ ТЕСТУВАННЯ СИСТЕМ З МІКРОСЕРВІСНОЮ АРХІТЕКТУРОЮ

Остапов О.А., Шевченко І.І., Чуб М.М.

Інститут телекомунікаційних систем КПІ ім.Ігоря Сікорського, Україна

E-mail: chub.mykhailo@lil.kpi.ua

Features of testing systems with microservice architecture

The current trend of creating web applications is based on the use of microservice architecture. The paper describes difficulties of testing microservices.

Одним з передових підходів створення інформаційних систем є використання мікросервісної архітектури інформаційної системи. Особливістю мікросервісної архітектури є те, що кожен сервіс розгортається незалежно від інших і реалізує виконання певної заданої функціональності системи, а отже данні зберігаються децентралізовано. Крім того, при використанні даного підходу для досягнення бізнес-потреб немає обмежень на вибір технології для реалізації кожного мікросервісу. Отже, мікросервіси - це декомпозицією великої бізнес-системи на незалежні елементи, які легко розгорнути і легко обслуговувати, при цьому кожен з них виконує одну певну задачу [1, 2].

Типовий життєвий цикл розробки програмного забезпечення складається з наступних фаз: збір і аналіз вимог (Requirement analysis), дизайн (Design) реалізація (Implementation), тестування (Testing), розгортання (Deployment) та підтримка (Maintenance). Тестування відповідає за забезпечення якісної роботи продукту, супроводжується перевіркою працездатності системи, виявленням, фіксацією і виправленням помилок з метою досягнення необхідних стандартів якості. Метою даної статті є огляд основних особливостей тестування систем з мікросервісною архітектурою по відношенню до систем з монолітною [3, 4].

Концепція монолітного програмного забезпечення розглядається як традиційний метод розробки додатків та полягає в тому, що різні компоненти програми об'єднуються в одну програму на одній платформі, а отже всі модулі, що відповідають за різну бізнес-логіку, вміщено в одній програмі та запущено в одному процесі.

Мікросервіси надають змогу виконувати ту ж саму роботу, що й моноліт, але розподіливши модулі в окремі віртуальні машини-контейнери за принципом «один модуль — одне завдання — один контейнер» і зв'язавши їх за допомогою віртуальної мережі [5].

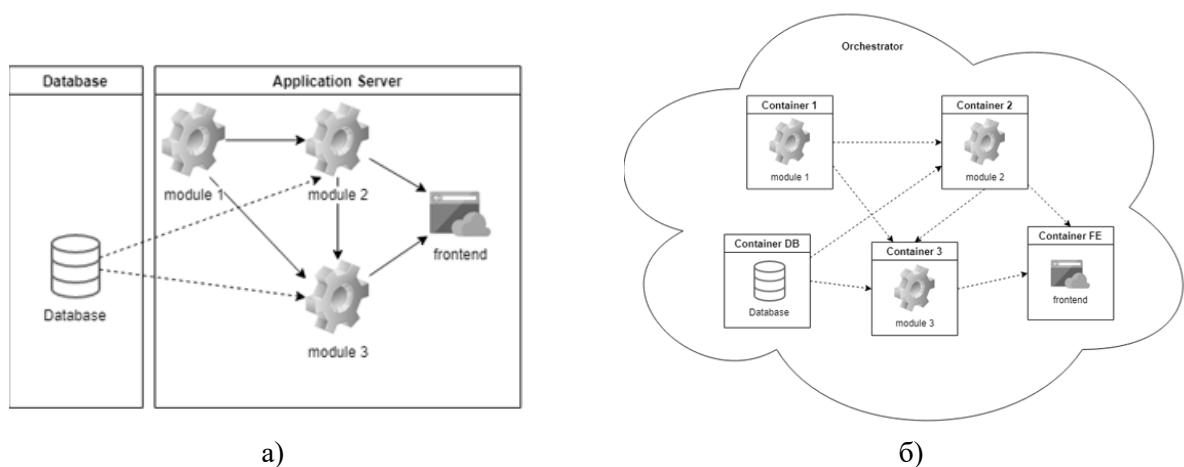


Рис.1. Архітектура програмного забезпечення: а) монолітна, б) мікросервісна.

Мікросервіси складно тестувати атомарно. В якості програмних інтерфейсів для взаємодії з мікросервісами, як правило, використовують RESTful API і асинхронний обмін повідомленнями через черги. При тестування веб-сервісів з визначеними наборами даних для монолітної архітектури достатньо локально розгорнути систему. У 99% випадків не можна запустити один окремий мікросервіс, щоб протестувати його REST веб-сервіси, наприклад, не створивши спочатку Mock-server всіх пов'язаних з ним сервісів, що унеможливорює інтеграційне тестування.

Кожен мікросервіс може мати свою окрему базу даних, ніяк не пов'язану з базами інших мікросервісів. З погляду автономності даний підхід є раціональним, але якщо об'єкти в системі, що тестуються, мають дочірні об'єкти кожного мікросервісу, база даних не може забезпечити їхньої цілісності. Рішенням є створення окремого механізму для зв'язності даних у кожному мікросервісі, наприклад, зберігати ID об'єктів інших сервісів. Проблема в тому, що дані одного мікросервісу можуть бути стерті, а помилку можна знайти лише на етапі тестування. Рішенням даної проблеми є створення та редагування даних через UI в невеликих обсягах під кожний конкретний тест.

Для мікросервісів важко забезпечити транзакційність. Тестування транзакцій у мікросервісах полягає в тому, що перший сервіс робить зміни в даних і передає їх другому сервісу — другий сервіс робить зміни у своїх даних і передає третьому. Під час такого тестування може виникнути помилка, наприклад, необробленого Null Pointer Exception. Тест не пройшов, дані перших двох мікросервісів не відповідають іншим — потрібно вручну їх чистити. Для забезпечення транзакційності між різними мікросервісами виникає необхідність розробникам писати більше коду, більше веб-сервісів для зворотного зв'язку, що потребує більше часу на тестування. З погляду цілої системи може бути зовсім не очевидно, в якому саме мікросервісі сталася помилка, для чого необхідно вручну перевіряти Log системи та данні

всіх залучених сервісів. У монолітах же транзакційність гарантують на рівні бази даних.

При монолітній архітектурі ПЗ може містити певну кількість веб-сервісів, створених для виконання бізнес-функцій програми. При мікросервісній архітектурі кількість веб-сервісів значно збільшується, оскільки, крім тих самих сервісів для виконання бізнес-функцій, додаються технічні сервіси для зв'язку мікросервісів між собою, які також потребують тестування. Кожен веб-сервіс одночасно повинен передавати більше даних (рис 2), а кожний новий канал комунікації ускладнює тестування й часто потребує встановлення спеціальних програм для роботи.

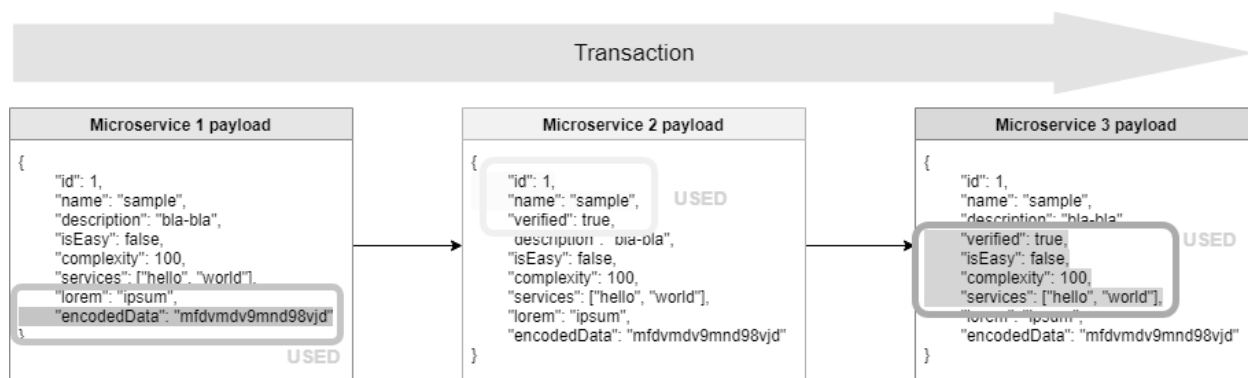


Рис.2. Передача даних при мікросервісній архітектурі.

Мікросервіси потребують значної кількості ресурсів, адже кожен контейнер мікросервісу - власна віртуальна машина, що використовує ресурси. У разі ж монолітної архітектури є лише один сервер чи віртуальна машина.

В роботі описано основні особливості та основні підходи до тестування програмного забезпечення з мікросервісною архітектурою.

Література

1. Ільченко М.Ю., Кравчук С.О. Телекомунікаційні системи. – К.: Наукова думка, 2017.
4. nergy efficiency analysis of hybrid-ARQ relay-assisted schemes in LTE-based systems nergy efficiency analysis of hybrid-ARQ relay-assisted schemes in LTE-based systems.
2. Кравчук С.О., Шевченко І.І., Чуб М.М. Технології, що можуть прискорити розвиток інфокомунікаційної галузі та становлення інформаційного суспільства// Матер. 13-ї міжнар. наук.-техн. конф. "Перспективи телекомунікацій", 15-19 квітня 2019 р. – К.: КПІ ім. Ігоря Сікорського, 2019. – С. 192–195.
3. Rajasekharaiah C. Microservices, Here and Beyond. In: Cloud-Based Microservices. Apress, Berkeley, CA., 2021 https://doi.org/10.1007/978-1-4842-6564-2_10.
4. Rao, P. V. , V. P.Kumar, and B. P. K.Reddy . 2018. "Applying Agile Software Methodology for the Development of Software Development Life Cycle Process (Sdlc)." Journal for Research— Volume 4 (2): 125–136.
5. G. Campeanu, "A mapping study on microservice architectures of internet of things and cloud computing solutions", 2018 7th Mediterranean Conference on Embedded Computing (MECO), pp. 1-4, June 2018.

ПРОТОКОЛ ЗАПОБІГАННЯ КОЛІЗІЙ В МЕРЕЖІ ІoT З ВИКОРИСТАННЯМ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Нагорна М.М., Кравчук С.О.

Інститут телекомунікаційних систем КІП ім. Ігоря Сікорського, Україна

E-mail: margarita.nagornaya999@gmail.com

COLLISION AVOIDANCE PROTOCOL IN THE IoT NETWORK USING DRONES

This article will discuss the IoT collision avoidance protocol using unmanned aerial vehicles. The principle of operation of the protocol is considered and compared with existing ones. The purpose of this protocol is to minimize the occurrence of collisions.

Ефективне впровадження технологій Інтернету речей (IoT) потребує задіяння нових технологій і підходів до створення телекомунікаційних мереж сенсорного спрямування. Одним із таких перспективних напрямків є задіяння безпілотних літальних апаратів та безпроводових технологій персонального і локального рівнів на базі радіочастотної ідентифікації (RFID). У порівнянні з іншими подібними автоматизованими технологіями ідентифікації, RFID має перевагу ідентифікації на великі відстані, малий обсяг, сильний захист від забруднень, велику ємність даних та високу надійність. Однак у щільному середовищі RFID, оскільки всі теги (радіочастотні мітки) мають один і той же безпроводовий канал, можливе накладання тегів – виникнення колізій. А використання кількох зчитувачів спричинить колізію між зчитувачами, що суттєво вплине на ефективність роботи IoT-систем.

Сценарій застосування безпілотного літального апарату (БПЛА), де можна призначати мітки, що можуть мати кілька частот, є шляхом для розв'язання цієї проблеми. Порівняно з традиційною системою RFID, система RFID на основі БПЛА має значно більше охоплення. Зчитувачі можуть ідентифікувати кілька тегів різної частоти в одному часовому інтервалі. На основі такої функції запропоновано алгоритм боротьби з колізією для IoT, названий протоколом протидії колізії для множини міток на основі безпілотних літаючих апаратів (ПКМ). Протокол ПКМ використовує зчитувач на основі БПЛА для ідентифікації мультичастотних міток з оптимальною ефективною системою, яка може ефективно вирішити проблему колізій міток для щільних середовищ IoT.

Базова система RFID, що складається з двох основних елементів: зчитувачів та міток використовує радіочастотні хвилі для зв'язку, теги завжди пасивні, і вони не можуть активно надсилати сигнали читачеві. Однак із збільшенням кількості міток та розширенням комунікаційних областей орієнтовані на майбутнє програми IoT повинні бути розумними, гнучкими та ефективними. Отже, поєднання БПЛА з RFID може легко реалізувати програми IoT за допомогою існування тривимірної моделі системи RFID, заснованої на БПЛА. Використання БЛА зменшить витрати та підвищить

ефективність, порівняно з використанням фіксованого зчитувача, як у першому випадку.

Система RFID використовує безпроводовий зв'язок для взаємодії інформації. Тому відбуватиметься колізія сигналів. Колізії міток призведуть до зниження ефективності ідентифікації системи RFID. Тому ключовим для системи RFID є вирішення проблеми ідентифікації з багатьма тегамі. Загалом, існує чотири рішення для вирішення проблеми зіткнення міток: (FDMA), (TDMA), (CMDA) та (SDMA). Серед них TDMA широко використовується протокол проти зіткнень. Однак, оскільки в один і той же часовий інтервал є декілька одночастотних відповідей тегів, TDMA не зможе правильно ідентифікувати тег. Передумова правильної ідентифікації тегів за допомогою TDMA полягає в тому, що в одному часовому інтервалі є лише одна відповідь тегу.

У щільних середовищах RFID, коли кількість міток збільшується, ймовірність виникнення колізій у каналі також збільшується. Якщо для зв'язку з пристроєм зчитування використовується одна мітка частоти, ефективність системи RFID значно знижується. Таким чином, у цій роботі ми розглядаємо систему RFID, яка включає зчитувач і багаточастотні мітки, і ми використовуємо багаточастотні мітки для зв'язку. У той же часовий інтервал зчитувач може ідентифікувати кілька міток різних частот. Колізії відбуватимуться лише тоді, коли мітки мають однакову робочу частоту і виходять на зв'язок в один і той же час.

Беручи до уваги ранні роботи щодо використовуваних підходів до запобігання виникнення колізій, слід зробити висновок, що, вони, як правило, базуються на традиційних протоколах уникнення колізій і не беруть до уваги характеристики щільних середовищ RFID, такі як висока щільність міток та сценарій тривимірного зв'язку та можуть не враховувати мобільність пристрою зчитування. В середовищі IoT часто використовується режим розпізнавання мобільних пристроїв. Отже, у цій роботі ми повністю розглядаємо метод зв'язку з багаточастотними мітками в IoT, який не вивчався раніше. І ми вводимо БПЛА в IoT, який може гнучко ідентифікувати теги в 3-D сценах. Це представляє інноваційне застосування IoT.

Інтерпретація протоколу протидії колізій множини міток на основі БПЛА, відбувається у поєднанні характеристики ефективності оптимальної системи та багаточастотного зв'язку. Протокол може надавати читачеві можливість читати більше тегів за той самий часовий інтервал. Протокол ПКМ в основному складається з двох етапів: отримання найкращої ефективності системи та досягнення багаточастотного зв'язку.

Ми визначаємо N тегів у системі для очікування ідентифікації та використовуємо TDMA для розподілу часових інтервалів. Довжина кадру часового інтервалу становить L . Відповідно до характеристик тегів у часовому інтервалі, ймовірність того, що n міток вибере той самий часовий інтервал, виглядає як

$$p(n) = C N n p n (1 - p) (N - n) \left(p = \frac{1}{L} \right) \quad (1)$$

На даний час максимальна довжина кадру може дорівнювати 256. Коли кількість тегів перевищує 256, ефективність системи неможливо збільшити за рахунок збільшення довжини фрейму. Теги групуються для досягнення найкращої ефективності розпізнавання в межах групи. У ПКМ ми використовуємо багаточастотні мітки для ідентифікації. У той же часовий інтервал читач може ідентифікувати мітки різних частот. Крім того, для спрощення результатів обчислення, ПКМ буде ігнорувати випадок, коли одночасно реагує більше тегів t в одному часовому інтервалі. Згідно з вищенаведеним аналізом, ефективність системи ПКМ можна розрахувати як

$$E_{system\ UMTAP} = \frac{S_{Snew}}{L} \quad (2)$$

Протокол ПКМ розробляється, користуючись перевагами DFSA. ПКМ може адаптивно та динамічно регулювати довжину кадру. Він обчислює кількість тегів, які слід ідентифікувати, відповідно до кількості тегів, успішно визначених у першому кадрі. Відповідно до результату оцінки та успішно ідентифікованих тегів у вихідному кадрі, зчитувач регулює довжину наступних кадрів, щоб виконати оптимальну ідентифікацію.

Для скорочення часу ідентифікації, ми розробили багаточастотні мітки для участі в ідентифікації. Таким чином, на основі багаточастотних міток зчитувач може ідентифікувати більше тегів з меншою кількістю часових інтервалів. Покриття зчитувача буде ширшим, що зменшить виникнення колізій зчитувач-зчитувач.

Для оцінки запропонованого антиколізійного протоколу (ПКМ), а саме аналізу ефективності системи та часу ідентифікації, було використано симулятор Matlab. таким як Pure Aloha (PA), Slot Aloha (SA), Frame Slot Aloha (FSA) та Dynamic FSA (DFSA). Результати демонструють, що запропонована схема MFPR може забезпечити кращі показники ефективності системи та часу ідентифікації.

За впливом різних частот міток на роботу протоколу було зроблено висновок про те, що ефективність системи всіх алгоритмів зростає із збільшенням кількості частот тегів. Причина в тому, що чим більше частот тегів, тим більше шансів їх ідентифікувати. Однак, оскільки частота мітки обмежена вартістю зчитувача та складністю зчитування, частота не може бути занадто великою.

Слід зазначити, що зі збільшенням довжини кадру зчитувача ефективність системи ПКМ зростає. Коли довжина кадру зчитувача дорівнює кількості міток, система RFID є найбільш ефективною. На даний момент максимальна ефективність нашої системи алгоритмів може досягати 69,1%, що значно покращить ефективність порівняно з існуючими відповідними алгоритмами. Також за критерієм впливу різної кількості тегів на роботу протоколу було виявлено, що у ПКМ, оскільки для ідентифікації використовуються багаточастотні мітки, теги різних частот можуть бути

ідентифіковані в одному часовому інтервалі, що упереджує таку проблему коли кількість тегів перевищує оптимальну довжину кадру, часовий інтервал зіткнення збільшується, і зчитувач не може розпізнати неідентифіковані теги. Також алгоритм має функцію групування міток, яка зменшує кількість міток, визначених групуванням, і може регулювати довжину кадру всередині групи. Загальна кількість часових інтервалів, необхідних для ПКМ, є найменшою, оскільки вона використовує оптимізований розмір кроку відповідно до групування, а довжина кадру динамічно регулюється з урахуванням кількості тегів у групі, щоб забезпечити високу ефективність ідентифікації системи в групі. Крім того, для розпізнавання використовуються багатоатрибутні теги, які можуть ідентифікувати більше тегів і зменшити часові інтервали зіткнень.

Результати моделювання показують, що схема MFPR має кращу продуктивність, ніж інші протоколи, що є результатом вдосконалення прийняття рішень за протоколом проти зіткнень. Виконуючи оцінку міток та використовуючи багаточастотні мітки, MFPR може зменшити часові інтервали зіткнення. Таким чином, MFPR досягає поліпшення продуктивності з точки зору ефективності системи та часу ідентифікації.

Отже, у даній роботі розроблено новий алгоритм боротьби із колізіями для IoT, який отримав назву протоколу протидії колізії множини тегів на базі БПЛА (ПКМ). В ПКМ було представлено тривимірну модель системи RFID на основі БПЛА, для ширшого охоплення спектру комунікацій та зменшення потреби в налаштуванні зчитувачів. Тоді протокол ПКМ використовує теги різної частоти для підключення до зчитувача, щоб зменшити часовий інтервал зіткнення. Одночасно ПКМ може досягти оптимальної ефективності системи, оцінюючи кількість тегів та динамічно регулюючи довжину кадру. Результати моделювання показують, що в порівнянні з традиційним протоколом проти зіткнень IoT алгоритм ПКМ забезпечує значне покращення продуктивності системи та часу ідентифікації.

Література

1. X. Jia, M. Bolic, Y. Feng, and Y. Gu, "An efficient dynamic anti-collision protocol for mobile rfid tags identification," *IEEE Communications Letters*, vol. 23, no. 4, pp. 620–623, Apr. 2019.
2. J. Su, Z. Sheng, L. Xie, G. Li, and A. X. Liu, "Fast splitting-based tag identification algorithm for anti-collision in uhf rfid system," *IEEE Transactions on Communications*, vol. 67, no. 3, pp. 2527–2538, Mar. 2019.
3. J. Zhang, X. Wang, Z. Yu, Y. Lyu, S. Mao, S. C. Periaswamy, J. Patton, and X. Wang, "Robust rfid based 6-dof localization for unmanned aerial vehicles," *IEEE Access*, vol. 7, pp. 77 348–77 361, 2019.
4. H. Wang, S. Pang, H. Zhang, and Q. Huang, "Aloha based anti-collision algorithm for rfid tag identification under capture environment," pp. 117–121, Aug. 2018.
5. L. Zhang, W. Xiang, X. Tang, Q. Li, and Q. Yan, "A time- and energy-aware collision tree protocol for efficient large-scale rfid tag identification," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2406–2417, Jun. 2018.

ЗАХИЩЕНА ВІД ВПЛИВУ НАВМИСНИХ ЗАВАД СИСТЕМА ЗВ'ЯЗКУ МАЛОГАБАРИТНИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Кайдено М.М.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: kkk610@ukr.net

PROTECTED FROM THE EFFECTS OF JAMMING COMMUNICATION SYSTEM OF SMALL-SIZED UAVs

This article describes the features of constructing a communication and control system of UAVs that is protected from the effects of deliberate interference. The structure of the UAV communication system and its features that provide protection against deliberate interference are presented.

На сьогоднішній день дослідженням в галузі створення систем зв'язку та управління безпілотних апаратів, захищених від впливу різноманітних завад, особливо навмисних, приділяється особлива увага вчених та інженерів в усьому світі. Навмисні завади можуть призводити до тимчасової втрати управління безпілотним апаратом, виведення його з ладу, перехоплення управління апаратом і, як наслідок, нецільового його використання. Найбільшу небезпеку несе нецільове використання безпілотного апарату зловмисниками, оскільки при цьому він може використовуватись як засіб для терористичних атак, наприклад на об'єкти підвищеної небезпеки.

В багатьох роботах відзначається, що безпека БПЛА є головною проблемою, особливо з точки зору кібератак і на даний час не існує типового способу його захисту від них. Зокрема роботи [1, 2] присвячені дослідженню стійкості комерційних та недорогих моделей БПЛА спеціального призначення, які використовують технологію WiFi для зв'язку та управління. Визначено значну вразливість таких БПЛА до кібератак, що можуть призводити до перехоплення та нецільового використання.

Окремі роботи, зокрема російських дослідників [3], присвячені не методам захисту БПЛА від навмисних завад, а навпаки методам протидії безпілотним апаратам шляхом створення в тому числі і різних видів навмисних завад. При цьому основний акцент робиться не просто на кібератаку на БПЛА, а на подавлення каналу зв'язку, або перехоплення безпілотного апарату шляхом підміни інформації в каналі управління.

В роботах [4, 5] було запропоновано архітектуру системи зв'язку безпілотного апарату для підвищення його живучості, яка досягається за рахунок застосування адаптації по діапазону частот з використанням додаткового каналу прийому для безперервного аналізу завадової обстановки, використанням двох та більше каналів передачі даних, складних алгоритмів оптимального вибору робочого діапазону, параметрів каналу передачі та адаптивних протоколів одночасної передачі даних по двом та більше каналам. Однак таке рішення не завжди може бути використано для

захисту малогабаритних БПЛА, оскільки основним обмеженням для застосування такої системи є обмеження на вагу корисного навантаження. Це обмеження призводить до того, що кількість бортової апаратури має бути мінімальною. При цьому використання двох каналів передачі потребує вдвічі більше енергетичних затрат, що призводить до необхідності збільшення ємності акумуляторної батареї.

Живучість безпілотного апарату з точки зору управління ним в першу чергу залежить від живучості системи зв'язку та управління, вихід з ладу якої призводить до повної втрати управління апаратом та, як наслідок до втрати самого апарату. За призначенням канал зв'язку від наземної станції до БПЛА є каналом управління, а канал зв'язку від БПЛА до наземної станції є каналом передачі телеметрії. В структурі системи зв'язку та управління безпілотного апарату, структура бортового обладнання якої показана на рис.1 використовується два канали прийому в двох фіксованих частотних діапазонах (як приклад для БПЛА цивільного використання 2,4 та 5,8 ГГц) та один канал передачі. Наземна станція зв'язку та управління БПЛА відповідно має два канали передачі та один канал прийому.

Використання частотного чи часового дуплексу відіграє також істотну роль в живучості каналу зв'язку. При частотному дуплексі канал передачі та прийому рознесені по частоті і тому визначення, на якій конкретній частоті працює канал управління БПЛА в точці перехоплення потребує істотно більшої чутливості приймача перехоплювача. При часовому дуплексі ж інформація про частоти роботи БПЛА легко може бути отримана перехоплювачем.

Використання одночасно двох каналів прийому з передачею повністю дубльованої інформації управління дозволяє істотно підвищити живучість каналу управління відносно енергетичної завади глушення каналу, оскільки для цього потребується або одночасна постановка енергетичної завади в двох діапазонах частот, або використання широкосмугової завади, для постановки якої використовуються станції постановки завад, вартість яких на порядки вища за вартість БПЛА, проти якого використовується така станція.

Для боротьби з завадами перехоплення та імітації каналу використовуються алгоритми виявлення імітаційних структурованих завад. Ці алгоритми базуються на синхронізації каналів, підтримці заданого рівня енергетики каналу та моніторингу енергетичних характеристик в каналах, маркуванням пакетів даних. Підтримка заданого рівня енергетики каналу, який повинен бути однаковим в обох каналах забезпечує додаткову скритність передачі інформації, знижуючи вірогідність перехоплення станцією, яка не знаходиться в зоні прямої видимості. Синхронізація каналів та підтримка заданого рівню енергетики реалізується шляхом використання технологій програмно-визначуваного радіо та систем на кристалі, описаних в [6].

Подавлення каналу телеметрії потребує більших енергетичних затрат від станції перехоплення, внаслідок того, що вона повинна розміщуватись набагато ближче до БПЛА, ніж до наземної станції управління. Тому нагальної необхідності в використанні двох каналів передачі немає. Не зважаючи на це, при використанні широкосмугового підсилювача потужності

можна комутувати виходи передавачів трансиверів з метою зміни діапазону частот каналу телеметрії.

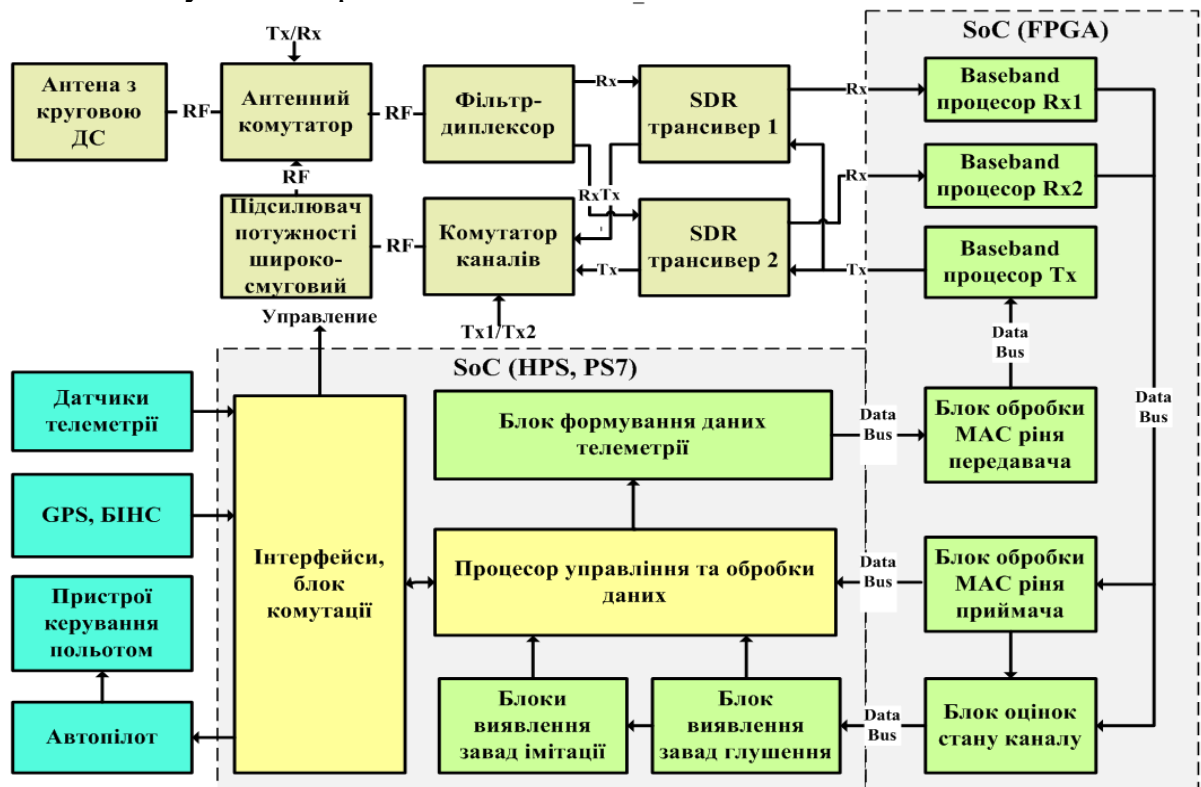


Рис.1. Структура бортового обладнання системи зв'язку та управління безпілотною апарату в режимі TDD.

Література

1. Carlos Augusto Tovar Bonilla, Octavio José Salcedo Parra, Jhon Hernán Díaz Forero. Common Security Attacks on Drones. International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 7 (2018) pp. 4982-4988 [<http://www.ripublication.com> 4982].
2. Hooper, M., Tian, Y., Zhou, R., Cao, B., Lauf, A., Watkins, L., Robinson, W., Alexis, W.: Securing commercial WiFi-based UAVs from common security attacks. In: MILCOM 2016—2016 IEEE Military Communications Conference (2016), [DOI: 10.1109/MILCOM.2016.7795496].
3. Теодорович Н.Н., Строганова С.М., Абрамов П.С. Способы обнаружения и борьбы с малогабаритными беспилотными летательными аппаратами // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 9, No1 (2017), [<http://naukovedenie.ru/PDF/13TVN117.pdf>].
4. M. Kaidenko and S. Kravchuk, "Creation of communication system for unmanned aerial vehicles using SDR and SOC technologies," 2019 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Odessa, Ukraine, 2019, pp. 1-4, [doi: 10.1109/UkrMiCo47782.2019.9165422].
5. Kaidenko M., Kravchuk S. (2021) Autonomous Unmanned Aerial Vehicles Communications on the Base of Software-Defined Radio. In: Ilchenko M., Uryvsky L., Globa L. (eds) Advances in Information and Communication Technology and Systems. MCT 2019. Lecture Notes in Networks and Systems, vol 152. Springer, Cham. [https://doi.org/10.1007/978-3-030-58359-0_16].
6. Kaidenko M.M., Roskoshnyi D.V. (2019) Software Defined Radio in Communications. 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 DOI, [https://doi.org/10.1007/978-3-030-16770-7_11 Print ISBN 978-3-030-16769-1].

МЕТОДИ І ТЕХНОЛОГІЇ ПОЗИЦІОНУВАННЯ ДЛЯ ВІРТУАЛЬНОЇ РЕАЛЬНОСТІ

Токаренко М.Я., Кравчук С. О.

Інститут телекомунікаційних систем КІП ім. Ігоря Сікорського, Україна

E-mail: matvey.tokarenko@gmail.com

METHODS AND TECHNOLOGIES OF POSITION TRACKING FOR VIRTUAL REALITY

This paper will contain the basic methods of virtual reality tracking and analysis of some models in purpose to find the best ideas and solutions

Незважаючи на те, що такому поняттю як віртуальна реальність вже більше 50 років, такі технології було абсолютно не вигідно розвивати у зв'язку з високими цінами на персональні ЕВМ та їх непристосованістю до роботи із 3D графікою. Все почало поступово змінюватися, коли у 2014 році на ринок вийшов перший масовий VR шолом Oculus Rift. З тих пір цей ринок невпинно зростає, оскільки електроніка стає дедалі масовою, а графіка - все кращою.

Звісно, така суміш технічних засобів накладає свої обмеження на реалізацію потенційної задачі. Одна з найголовніших хвороб VR шоломів – коректне і швидке позиціонування відносно реального простору. Із зростанням можливостей персональних комп'ютерів зростають і примхи користувачів щодо якості контенту. Це доволі молода галузь, тому єдиних стандартів в ній не існує, а кожна компанія, що займається розробкою VR систем не прагне ділитися своїми напрацюваннями із потенційними конкурентами.

Метою даної роботи є дослідження основних методів позиціонування VR систем у просторі, безпосередній аналіз існуючих комерційних VR шоломів та виокремлення основних моментів, що можуть сприяти подальшому розвитку таких систем.

Базовими методами є акустичні, радіочастотні, магнітні, оптичні, та інерційні. Будь який гібридний метод є лише певною комбінацією вищезазначених методів. Людське сприйняття пред'являє високі вимоги до точності (~ 1 мм) і затримок (< 20 мс) в ВР обладнанні. Розглянемо базові принципи, на яких побудовані перераховані вище методи.:

Акустичні методи використовують ультразвукові хвилі для виміру положення і орієнтації цільового об'єкта. Для визначення положення об'єкта вимірюється час прольоту звукової хвилі від передавача до приймачів або

різниця фаз синусоїдальної звукової хвилі при прийому-передачі. Акустичні трекери, як правило, мають низьку швидкість оновлення, викликану низькою швидкістю звуку в повітрі. радіочастотні методи

Методів заснованих на радіочастотах безліч. Багато в чому за принципами визначення положення вони схожі з акустичними методами відстеження (відмінність лише в природі хвилі

Магнітний трекінг заснований на вимірюванні інтенсивності магнітного поля в різних напрямках. Як правило, в таких системах є базова станція, яка генерує змінне або постійне магнітне поле. Так як сила магнітного поля зменшується зі збільшенням відстані між точкою вимірювання і базовою станцією, можна визначити місце розташування контролера. Якщо точка вимірювання обертається, розподіл магнітного поля змінюється за різними осях, що дозволяє визначити орієнтацію.

Оптичні методи являють собою сукупність алгоритмів комп'ютерного зору і відстежують пристрої, в ролі яких виступають камери видимого або інфрачервоного діапазону, стерео-камери і камери глибини.

Залежно від вибору системи відліку виділяють два підходи для відстеження положення:

Outside-in підхід має на увазі присутність нерухомого зовнішнього спостерігача (камера), що визначає положення рухомого об'єкту по характерних точках. Використовується в Oculus Rift (Constellation), PSVR, OSVR і безлічі Motion Capture систем.

Inside-out підхід передбачає наявність на об'єкті, що рухається оптичного сенсора, завдяки якому можливо відслідковувати рух щодо нерухомих точок в навколишньому просторі. Використовується в Microsoft Hololens, Project Tango (SLAM), SteamVR Lighthouse (гібридний варіант, тому що є базові станції).

Література

1. Choi, SangSu, Kiwook Jung, and Sang Do Noh (2015). "Virtual reality applications in manufacturing industries: Past research, present findings, and future directions". *Concurrent Engineering*. 1063293X14568814.
2. Кармадонов В.Ю. "Методы отслеживания положения в виртуальной реальности" Журнал 'Academy' 2019.
3. The Complete Guide to Virtual Reality and the VR Industry. 'The Guardian' 2016.

АНАЛІЗ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СЕРВІСІВ MPLS VPN

Тимофєєв Є.М., Созонник Г.Д.

Національний технічний університет України

“Київський політехнічний інститут імені Ігоря Сікорського”

E-mail: timofeevzh@gmail.com

SECURITY ANALYSIS OF MPLS VPN SERVICES

Analyzes modern technologies to ensure the security of the service of building virtual private networks, technical solutions of VPN technologies on the example of the organization of a private virtual network based on MPLS network. Reasons for the need to protect against attack. The technique of complex data protection of the enterprise at the organization of VPN security service is offered.

Здійснено аналіз сучасних технологій щодо надання безпеки сервісу побудови віртуальних приватних мереж, технічних рішень технології VPN на прикладі організації приватної віртуальної мережі на основі мережі MPLS. Встановлено причини необхідності захисту від атак. Запропоновано методику комплексного захисту даних підприємства при організації безпечного сервісу VPN.

VPN (Virtual Private Network – віртуальна приватна мережа) – це приватна мережа, побудована в рамках загальнодоступної мережевої інфраструктури, такої як глобальний Інтернет. VPN означає не тільки ізоляцію комунікацій, а скоріше контрольоване сегментування для спільнот, що становлять інтерес, через спільну інфраструктуру. Технологія VPN стала однією з найважливіших послуг у транснаціональних компаніях по всьому світу завдяки своїй безпеці, зручності та низькій вартості розгортання [1].

MPLS (Multiprotocol Label Switching – багатопроTOCOLьна комутація по мітках) є основною магістральною технологією нового століття.

Технологія, заснована на MPLS VPN, базується на чіткому розмежуванні між постачальником послуг мережі (Р-мережа) та мережі споживача (С-мережа), як показано на рисунку 1 [2]. У порівнянні з традиційною технологією VPN, MPLS VPN є справді хорошим рішенням і має свої технологічні особливості та функції, такі як FEC, VRF, MPBGP, VPNv4-адреса тощо для подолання недоліків власне тунелювання.

Найважливішою характеристикою будь-якої системи передачі, незалежно від її складності і призначення, є безпека циркулюючої в ній інформації. Високий ступінь автоматизації, до якої прагне людство, широке впровадження дешевих комп'ютерних систем масового застосування та попиту роблять їх надзвичайно вразливими по відношенню до деструктивних дій, ставлять сучасне суспільство в залежність від ступеня безпеки

використовуваних інформаційних технологій. Загальна комп'ютеризація несе з собою численні проблеми, найбільш складною з яких є проблема інформаційної безпеки.

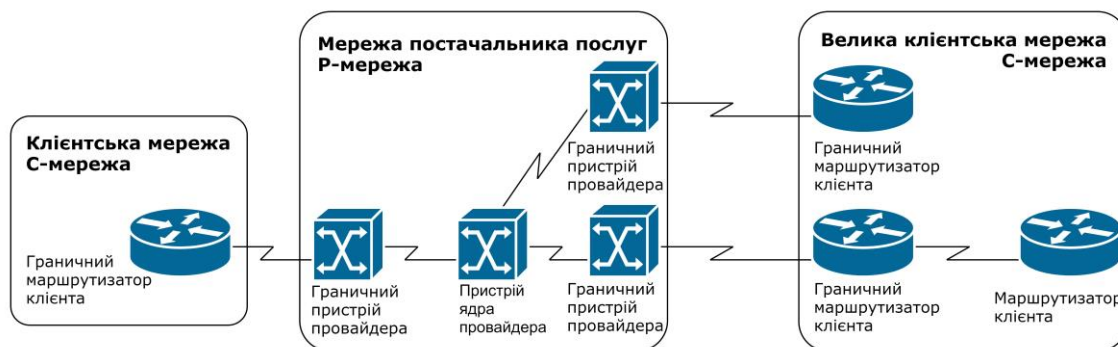


Рис.1. Мережа постачальника послуг та клієнтів на основі MPLS.

Мета створення систем безпеки – попередження або оперативне усунення наслідків умисних (навмисних) і випадкових деструктивних впливів, наслідком яких можуть бути руйнування, модифікація або витік інформації, а також дезінформація [3].

Критерієм при прийнятті будь-якого рішення щодо систем безпеки є цінність інформації. При цьому розрізняють чотири види загроз:

1. Викрадення інформації: проникнення в приватну мережу для отримання конфіденційної інформації, яка може бути використана або продана з різними цілями. Приклад: розкрадання конфіденційної інформації, що належить організації, наприклад, відомості про науково-технічні розробки.

2. Крадіжка особистої інформації для подальшого її використання. Використовуючи викрадені дані можна отримати юридичні документи, подати заяву на кредит та здійснити несанкціоновані покупки через Інтернет [4]. Проблема крадіжки особистої інформації продовжує загострюватися, а фінансові втрати становлять мільярди доларів в рік.

3. Втрата даних або маніпуляція даними: проникнення з метою знищення або зміни записів даних. Приклади втрати даних: передача вірусу, що «затирає» жорсткий диск комп'ютера. Приклад неправомірного використання даних - проникнення в систему зберігання даних з метою зміни даних, наприклад ціни виробу.

4. Припинення обслуговування: заборона доступу правомочних користувачів до служб, для використання яких їм має бути надане право. Приклад: атаки типу «відмова в обслуговуванні» (DoS-атаки) на сервери, мережеві пристрої і канали обміну даними по мережі.

Таким чином, навіть у невеликих мережах необхідно враховувати загрози безпеці та вразливості при плануванні впровадження мережі.

Для створення захищеного каналу VPN використовуються процедури

шифрування, аутентифікації і авторизації. Методів шифрування досить багато, тому важливо, щоб на кінцях тунелю використовувався один і той же алгоритм шифрування. Крім того, для успішного дешифрування даних джерела і одержувача даних необхідний обмін ключами шифрування. Під аутентифікацією розуміється визначення користувача або кінцевого пристрою. Аутентифікація дозволяє встановлювати з'єднання лише між легальними користувачами і, відповідно, запобігає доступ до ресурсів мережі несанкціонованих користувачів. У процедурі беруть участь дві сторони: одна доводить свою аутентичність, а інша її перевіряє і приймає рішення. Найчастіше для аутентифікації використовується пароль, але можуть застосовуватися інші докази. Недоліками застосування паролів є їх розкриття, що пояснюється їх простотою. Аутентифікація даних свідчить про їх цілісність, а також про те, що вони надійшли від одного з користувачів. Авторизація передбачає надання абонентам різних видів послуг. Кожному користувачеві надаються певні адміністратором права доступу. Ця процедура виконується після процедури аутентифікації і дозволяє контролювати доступ санкціонованих користувачів до ресурсів мережі. Взагалі, процедури аутентифікації і авторизації виконують одну задачу і до них пред'являються однакові вимоги. Цілісність переданих даних дозволяє забезпечити застосування електронного підпису.

Для забезпечення комплексного захисту інформації підприємства пропонується наступна стратегія: забезпечення безпечного доступу у будь-який час співробітників підприємства до мережевих ресурсів; забезпечення протидії атакам на DHCP сервер; впровадження в мережі функції IP Source Guard та DAI; забезпечення запобігання переповненню CAM таблиць комутаторів; використання мережевого екрану; організація Site-to-Site IPsec VPN зв'язку.

Висновок. Розглянуто сучасні методи організації безпеки віртуальних приватних мереж на основі MPLS. Описано процес створення захищеного VPN каналу та процедур шифрування, аутентифікації і авторизації. Запропонована методика комплексного підходу для забезпечення безпеки інформації підприємства.

Література

1. P. Ferguson, G. Huston, What is a VPN? Internet, <https://www.potaroo.net/papers/vpn.pdf>, April 1998.
2. I. Pepelnjak, J. Guichard, J. Aparcar, MPLS and VPN Architectures, Volume II. Cisco Press, 2003.
3. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. М.: Кудиц - Образ, 2001. — 363 с.
4. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс: учеб. пособие / А. Н. Андрончик, А. С. Коллеров, Н. И. Синадский, М. Ю. Щербаков; под общ. ред. Н. И. Синадского. – Екатеринбург: Изд-во Урал. ун-та, 2016. – 180с.

АНАЛІЗ ВИКОРИСТАННЯ ПРОТОКОЛІВ IPSEC ТА SSL В КОРПОРАТИВНИХ МЕРЕЖАХ

Корман Н.А., Могилевич Д.І.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail:kormannatasha21292@gmail.com

ANALYSIS OF THE USE OF IPSEC AND SSL PROTOCOLS IN CORPORATE NETWORKS

The use of IPsec and SSL protocols to increase the level of information security in corporate networks is analyzed, the main advantages and disadvantages of these protocols are investigated the analysis of the main problems of network information security in building a virtual network is analyzed.

Проаналізовано використання протоколів IPsec та SSL для підвищення рівня інформаційної безпеки в корпоративних мережах, досліджено основні проблеми мережевої інформаційної безпеки при побудові віртуальної корпоративної мережі.

Реалізувати віртуальну приватну мережу можна різними методами. Головною метою вибору способу побудови є її продуктивність та швидкість, сумісність між сайтами і компаніями, а також необхідність підтримувати багато типів мережевих профілів зв'язку, адже неправильна побудова може зупинити роботу мережі, через малопотужність маршрутизаторів, технічні конфлікти, політичні проблеми і проблема технічного досвіду, пов'язаними з будь-яким рішенням тому найкраще використовувати спеціалізоване обладнання або програмне рішення.

Основними способами реалізації VPN є:

1. Remote access VPN
2. Site-to-site VPN

Саме реалізація за допомогою VPN з мережею "мережа - віддалений користувач" відповідає за криптографічний захист, шифрування та дешифрування даних, що передаються.

З точки зору використовуваних протоколів можна виділити кілька типів Remote Access VPN:

- використовують протоколи сімейства IPsec / IKE;
- використовують протоколи сімейства SSL / TLS;
- використовують неліцензійні та незареєстровані протоколи, що несумісні з іншими рішеннями.

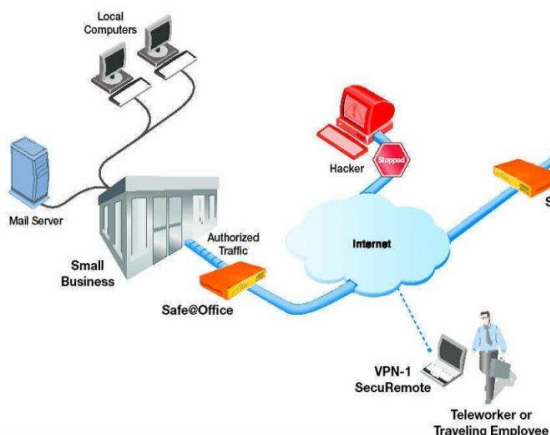


Рис. 1. Загальна схема підключення Remote access VPN.

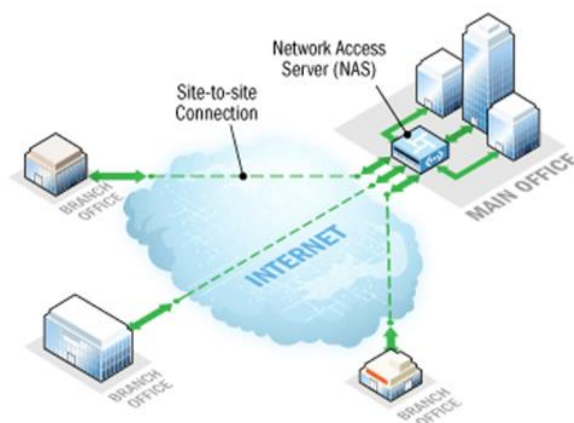


Рис. 2. Технічна реалізація VPN site-to-site.

Дані, що передаються спочатку переобразуються та шифруються VPN з віддаленим доступом, а вже тоді преєдається на шлюз, що розташований поза локальною мережею. Після надходження даних до шлюзу, вони підлягають дешифруванню і ретрансляції в локальну мережу.

Site-to-site VPN – реалізація в локальних мережах захищеного тунелю за допомогою двох маршрутизаторів для передачі даних без використання програмного забезпечення.

Існує два поширені типи VPN від сайту до сайту: інтранет та екстранет. VPN, що базуються на екстранеті, дозволяють компанії використовувати загальнодоступний Інтернет для підключення своєї локальної мережі до мереж інших фірм. Це надає змогу пересилати дані з інших будівель, зберігаючи свою локальну мережу (intranet).

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 через Інтернет. Він працює шляхом створення захищеного каналу між браузером користувача та сайтом, який користувач збирається відвідати. Будь-яка інформація відправлена по цьому каналу шифрується з одного боку і розшифровується одержувачем на іншій стороні.

Для підвищення захисту віртуальних приватних мереж на основі шифрування можна застосувати разом з технологіями VPN на основі розмежування трафіку. Технологія розмежування трафіку неодноразово

критикувалася за ненадійність безпеки, однак на сьогодні дана проблема має способи вирішення наприклад, за допомогою мережі VPN на основі протоколів IPSec и SSL.

Широкої популярності набуває побудова VPN на основі протоколу SSL(Secure Sockets Layer) та TLS(Transport Layer Security). SSL VPN будується за допомогою криптографічних методів шифрування інформації, що надає безпечний доступ з вашого персонального ПК до різних серверів Internet-додатків. Це відбувається завдяки тому, що веб-браузери вже інтегровані під SSL, такий захист даних має не тільки надійність, а й простоту реалізації, адже не потребує постійних налаштувань від користувача.

IPSec - це набір різних відкритих алгоритмів шифрування даних, що працюють поверх стека IP. Він надає служби аутентифікації і шифрування даних на мережевому рівні і може бути представлений на будь-якому пристрої, який працює по протоколу IP. Щоб домогтися конфіденційності передачі використовують два головних протоколи безпеки, такі як заголовок аутентифікації (AH- Authentication Header) та інкапсуляції пакетів (ESP- Encapsulating Security Payload), та протоколів обміну криптографічними ключами через мережу Internet (IKE-Internet Key Exchange), що забезпечують режим роботи в захищеному вигляді. Існує два основних режими для передачі пакетів даних між двома різними мережами, з якими працює IPsec VPN. Режим транспортування та тунелювання. Саме в першому режимі усі дані підтягаються шифруванню та передаються параметри захисту у заголовку IP-протоколу, у режимі тунелювання інкапсулюється увесь пакет даних, який і є носієм параметрів захисту. Протокол IPSec надає можливість виконувати наступні дії:

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

Популярність даний протокол отримав через свою простоту використання, та максимальну надійність, адже він інкапсулює передані дані двічі, це суттєво зменшує його швидкодію, у порівнянні з SSL OpenVPN або SSTP.

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.

Розглядаючи деякі основні моменти, що стосуються протоколу мережевої безпеки IPSec, можна зробити висновок, що протокол IPSec домінує в більшості реалізацій віртуальних приватних мереж.

Таблиця 1. Порівняльна характеристика IPsec та SSL.

Технологія	IPSec	SSL
Апаратна залежність	Так	Так
Код	Не потребує змін для додатків. Може вимагати доступ до 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.

Висновки. На сьогоднішній день найбільш надійними є протоколи IPsec та SSL, але пріоритетність використання даних протоколів для побудови VPN залежить від конкретних критеріїв (необхідний тип доступу для користувачів, рівень мережевої безпеки, рівень захисту даних, необхідність масштабованості мережі в майбутньому). Проаналізувавши основні моменти, що стосуються протоколу мережевої безпеки IPsec можна відзначити, що даний протокол домінує в більшості реалізацій віртуальних приватних мереж через подвійну інкапсуляцію даних. Отже, метою подальших досліджень є удосконалення методів побудови захищених з'єднань за допомогою протоколу IPSEC за схемами «точка-точка» і «мережа-мережа».

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> (дата звернення: 28.02.2021).
2. «Концепція захищених віртуальних приватних мереж»- Електронний ресурс. – Режим доступу: <https://stud.com.ua/97437>(дата звернення: 04.03.2021).
3. Захист інформації. Криптографічні методи : Підруч. для вищ. навч. закл. / І.І. Маракова, А.І. Рибак, Ю.С. Ямпольський; Одес. держ. Політехн. ун-т, Ін-т радіоелектрон. і телекомунікацій. - О., 2001. - 174 с. (дата звернення: 01.03.2021).
4. Биячув Т. БЕЗПЕКА КОРПОРАТИВНИХ МЕРЕЖ / Т.А. Биячув. – СПб: СПб ДУ ІТМО, 2004. – 161 с.(дата звернення: 04.03.2021).
5. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети - анализ технологий и синтез решений. М.: ДМК Пресс, 2004. (дата звернення: 04.02.2021).
6. «What is difference between SSL VPN and IPsec VPN» - Електронний ресурс. – Режим доступу: <https://uk.gadget-info.com/57085-vpn-pros-and-cons-you-should-consider-before-using-it> (дата звернення: 28.02.2021).

QOS АНАЛІЗ МЕРЕЖ ПЕРЕДАЧІ ДАНИХ НА ОСНОВІ НЕЧІТКОЇ БАЗИ ЗНАНЬ

Глоба Л.С., Савчук З.Р.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: savchukzahar33@gmail.com

QOS ANALYSIS OF DATA TRANSMISSION NETWORKS BASED ON A FUZZY KNOWLEDGE BASE

This study proposes a method that increases the efficiency of the analysis of the telecommunications system by building a fuzzy knowledge base of statistical data sets in the form of logical structured rules, checking their reliability with a metagraph, which reduces the computational complexity of monitoring systems algorithms.

В даному дослідженні пропонується метод, який підвищує ефективність проведення аналізу роботи телекомунікаційної системи за рахунок побудови бази нечітких знань із статистичних наборів даних у вигляді логічних структурованих правил, проведення їх перевірки на достовірність за допомогою метаграфа, що дозволяє зменшити обчислювальну складність алгоритмів систем моніторингу.

Сучасні інформаційно-комунікаційні системи в поєднанні з новітніми 5G і 6G технологіями постійно трансформуються і розвиваються для збору, зберігання, обробки і передачі великих обсягів даних. Глобальний характер цих процесів вимагає дотримання заданих показників QoS, що в свою чергу потребує використання математичних методів обробки інформації для отримання корисних, необхідних і актуальних знань. Для гнучкості міркувань часто використовуються математичні методи нечітких множин, так як вони допомагають врахувати всі невизначеності, пов'язані з приналежністю об'єкта до певної множини. Для цього системи нечіткого виводу містять базу нечітких правил, що використовуються для реалізації нечіткого виводу [1,6]. Водночас за наявності значної кількості нечітких логічних правил у базі знань виникають конфлікти через неузгодженість таких правил, що потребує значних зусиль експертів. Це твердження говорить про те, що математичні методи нечіткої логіки в поєднанні з візуалізацією даних більш ефективні для моделей динамічних процесів таких, які відбуваються в телеком мережах під час передавання інформації.

Для перетворення вибірки даних у формат правил і подальшої роботи над ними використовується поетапний підхід:

1. Попередня обробка наборів даних застосовує попереднє очищення даних від випадково виникаючих помилок, використовуючи поєднання існуючих ефективних підходів у єдиний алгоритм, який динамічно

аналізує дані та визначає необхідні типи очистки.

2. Побудова нечітких логічних правил, використовуючи алгоритми кластеризації.
3. Очищення масиву правил бази нечітких знань від дублікатів та конфліктів.

На вхід алгоритму нечіткого логічного висновку подаються вхідні змінні, які несуть інформацію, отриману шляхом вимірювання деякої фізичної величини (система моніторингу телеком оператора). На виході алгоритму формуються підсумкові змінні нечіткого логічного висновку, наприклад рівень задоволеності якістю обслуговування.

Алгоритм нечіткого логічного висновку виконує перетворення значень вхідних змінних процесу моніторингу у вихідні змінні на основі певних нечітких правил продукції. Для перевірки запропонованого підходу використовувалися дані, що були отримані від одного з українських телеком операторів. Натуральні величини нормувалися в діапазоні від 0 до 1.

Для підвищення достовірності результату під час обробки великих обчислюваних даних за рахунок очищення даних від випадково виникаючих помилок застосовується перший крок [2]. Наступним етапом є формування БНЗ, де відбувається перетворення числових значень на терми лінгвістичних змінних, де використовуються функції приналежності отримані на етапі побудови функцій приналежності з кластерів [3]. Для терму відповідної лінгвістичної змінної для кожного числового значення з набору статистичних даних проводилася процедура «мапінгу» цих даних у відповідні терми. Значення відносяться до термів за рахунок їх приналежності до того чи іншого кластера. Вихідні дані виглядатимуть наступним чином (Таблиця 1).

Таблиця 1. Приклад бази нечітких знань з даних телеком оператора.

X ₁	X ₂	X ₃	X ₄	X ₅	X ₆	...	X ₁₂
середня	не низька	низька	не низька	не низька	середня	...	не низька
середня	середня	висока	середня	не низька	не низька	...	низька
...	...	...	...	...	...	...	...

Потрібно звернути увагу на те, що на даному кроці перетворення даних в терми лінгвістичних змінних можуть сформуватися конфліктуючі і дублюючі правила, через різну природу даних, або дані при кластеризації не правильно розподілилися між кластерами на границях розподілу.

На етапі реорганізації БНЗ, нечіткі логічні правила подаються як колекція пар двомірного масиву об'єктів у форматі «ім'я: значення». На першому етапі механізму очищення правил відбувається видалення дублікатів і додавання нової властивості weight (вага), яка відображає

частоту знаходження правила в проміжному наборі. Після чого відбувається очищення колекції правил від конфлікуючих правил, де проводиться перевірка лівої частини правила (Якщо...) на дублікат. Якщо існують два або більше однакових частин правила у яких значення результату суперечать одне одному, то вибирається той об'єкт, у якого параметр *weight* має більше значення і воно замінюється на середнє арифметичне всіх ваг конфлікуючих правил. Кінцевим результатом механізму очищення правил буде унікальний масив колекції об'єктів без аномалій із зазначеною вагою впливу правила на роботу системи підтримки прийняття рішення.

Перед початком виконанням реалізації побудови метаграфу, для файлу із очищеними правилами проводиться додаткова автоматична процедура форматування правил по принципу *nodes* та *links*, де *links* обов'язково визначає “source” і “target”, що вказують на напрям залежності об'єктів правил, а також параметр “value” що визначає вагу правила серед усіх правил бази нечітких знань [4]. На виході системи отримаємо готовий метаграф, за допомогою якого можна наочно редагувати логічні структури, визначати та аналізувати його властивості, які було б важко виявити, використовуючи текстове подання (див. рис. 1-2).

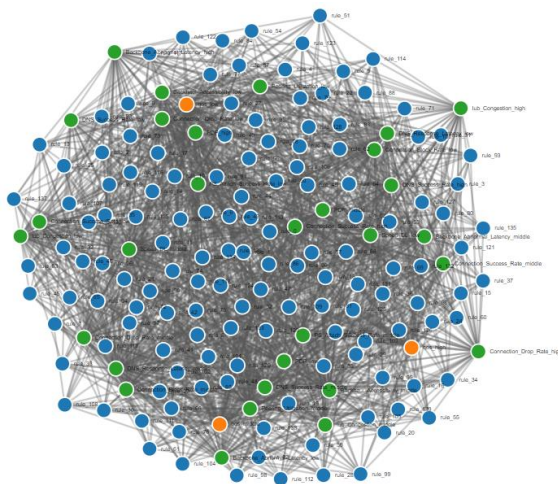


Рис. 1. Подання готового метаграфу.

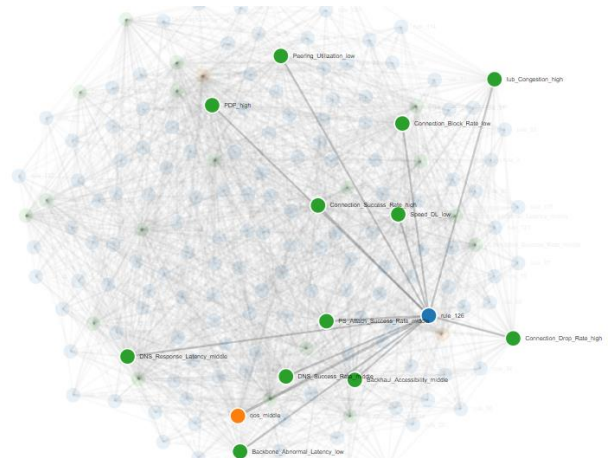


Рис. 2. Представлення окремого правила.

Як видно із рисунку 1 було побудовано метаграф на основі правил продукцій бази нечітких знань побудованої для українського телеком оператора, де виділяються три групи вершин: множина вершин, що відповідають термам в лівій частині правил (зелений); множина метавершин, що включають в собі вершини, відповідні термам з лівої частини правила (синій); множина вершин, що відповідають результуючим термам (оранжевий). На рисунку 2 виділено окреме правило, де значення параметру “value” представлено у вигляді ширини дуги, що з’єднує результуючий терм

та метавершину – чим більша ширина дуги, тим більший вплив правила на систему. Метаграф можна вважати, як вирішення проблеми прогнозування середньо- та велико-розмірних зв'язків, в якому мета полягає в точному навчанні моделей, які швидко адаптуються до нових даних [5]. Представлений метод візуалізації в порівнянні з іншими алгоритмами структуризації інформації можна вважати новим продуктивним методом графічного аналізу складних логічних структур, оскільки він дозволяє підвищити якість та достовірність отриманих нечітких логічних правил, що знаходяться у базі нечітких знань.

Висновки. В даному дослідженні запропоновано метод, який зменшує обчислювальну складність алгоритмів систем моніторингу оператора зв'язку за рахунок побудови бази нечітких знань із статистичних наборів даних у вигляді логічних структурованих правил з перевіркою на достовірність засобами апарату теорії метаграфа. Для перевірки можливості застосування даного методу була проведена побудова БНЗ із використанням даних одного з українських операторів зв'язку. Якість та достовірність нечітких логічних правил, вплив кожного параметра на QoS в цілому представлена як ширина дуги метаграфа. Представлений метод візуалізації в порівнянні з іншими алгоритмами структуризації інформації можна вважати новим продуктивним методом графічного аналізу складних логічних структур. Подальші дослідження плануються направити на створення системи моніторингу на базі запропонованого методу для 5G мереж.

Література

1. Altunin A.E. Models and algorithms for decision making in fuzzy conditions / A.E. Altunin, M.V. Semukhin. Tyumen: Tyumen State University, 2000. – 352 p. [in Russian].
2. Grebinichenko M.V. Methods of pre-processing of large data / M.V. Grebinichenko. Kyiv, 2020. – 54 p. [in Ukrainian].
3. Lyashenko A.V. Method of construction of fuzzy logical rules for big data / A.V. Lyashenko. Kyiv, 2020. – 67 p. [in Ukrainian]
4. Savchuk Z.R. Application of fuzzy logical rules for analysis and structuring of big data / Z.R. Savchuk. Kyiv, 2020. – 80 p. [in Ukrainian].
5. Savchuk Z.R. Means of visualization of complex logical structures / Z.R. Savchuk. //Proceedings of the International Scientific and Technical Conference "Prospects for Telecommunications". 15-19 April 2019, pp. 261-263. [in Ukrainian].
6. Piegat A. Fuzzy Modeling and Control / A. Piegat. – 2nd edition. – Moscow: BINOM. Knowledge Laboratory, 2018. – 798 p. [in Russian].

ПІДХІД ДО ДОСЛІДЖЕННЯ ПСИХОФІЗІОЛОГІЧНОГО СТАНУ ЛЮДИНИ НА ОСНОВІ МЕТОДІВ МАШИННОГО НАВЧАННЯ

Копа Р.В., Штогріна О.С.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: roma.kpv@gmail.com

APPROACH TO THE RESEARCH OF THE PSYCHOPHYSIOLOGICAL STATE OF HUMAN ON THE MACHINE LEARNING METHODS

This article describes the impact of extreme conditions on the psychophysiological state of human. A new approach to the research of the psychophysiological state of human is proposed, which allows to predict the human condition on the basis of machine learning methods. The efficiency of models for forecasting the assessment of human condition on the basis of different methods of machine learning is compared.

Загалом Антарктида завдяки міжнародним угодам про її охорону є лабораторією наукових досліджень. Антарктична станція «Академік Вернадський» – являється єдиною українською науковою установою, що діє на Антарктиді. Дослідження які проводять науковці можуть широко використовуватись в прогнозуванні зміні клімату, розвідці корисних копалин. Одна експедиція на станцію триває цілий рік при цьому зимівники які входять до неї потрапляють в екстремальні умови. Зимівники протягом довгого періоду перебувають в специфічному оточенні де у них фіксується велика кількість випадків порушень нормального режиму сну, симптомів головного болю, погіршення настрою і самопочуття [1]. Дані випадки погіршення стану людини сприяють зростанню ризику порушення психофізіологічного стану зимівників.

Наразі, в НАНЦ України активно ведуться дослідження психофізіологічного стану людини методами на основі кольорової преференції. Методи на основі кольорової преференції являються громіздкими та потребую досвіду роботи з даними [2]. Тому доцільно розробити підхід до аналізу психофізіологічного стану, який здатний прогнозувати оцінку стану людини на основі проходження тесту кольорової преференції.

НАНЦ України надав набір даних з пройденими тестам кольорової преференції, а також данні про суб'єктивне відчуття зимівників на основі яких можливо вирішити поставлену задачу. Використання методів машинного навчання поширене при роботі з великим набором даних, тому

що вони показують достатньо високу точність отриманих даних на виході [3], тому їх було використано при розробці підходу до аналізу психофізіологічного стану людини. Для вирішення задачі прогнозування стану людини було досліджено ефективність різних методів машинного навчання для задачі регресії: лінійна регресія (LR), регресія опорних векторів (SVR), метод к-найближчих сусідів (KNN), регресійне дерево (DT), на основі яких відбувається прогнозування стану людини.

Вхідні дані:

- тести кольорової преференції;
- еталонне значення кольорової преференції.

Вихідні дані:

- оцінка стану людини, яка базується на суб'єктивних відчуттях.

Для оцінки ефективності методів навчання будемо використовувати наступні метрики: коефіцієнт детермінації (рис. 1), середньоквадратична помилка (рис. 2), середня абсолютна помилка (рис. 3).

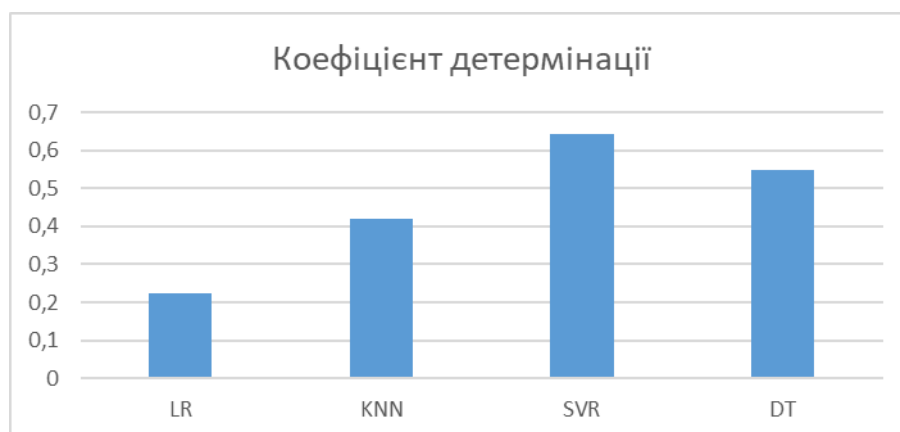


Рис. 1. Коефіцієнти детермінації для моделей на основі різних методів машинного навчання.

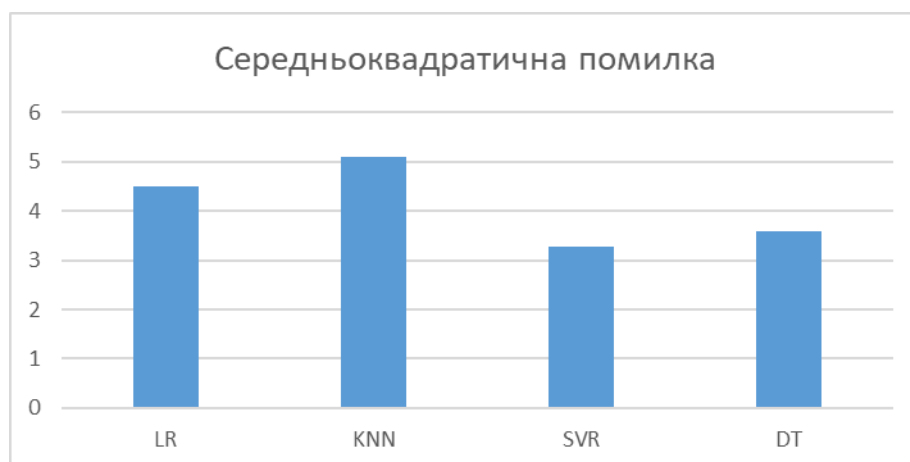


Рис. 2. Середньоквадратична помилка для моделей на основі різних методів машинного навчання.

Як видно з гістограм найкращим методом для навчання моделі виявився метод опорних векторів оскільки має найкращі коефіцієнт детермінації та найменшу середньоквадратичну помилку. Недоліком даного методу являється те, що потрібно підбирати параметри для моделі, та проводити нормалізацію даних які подаються на вхід моделі.

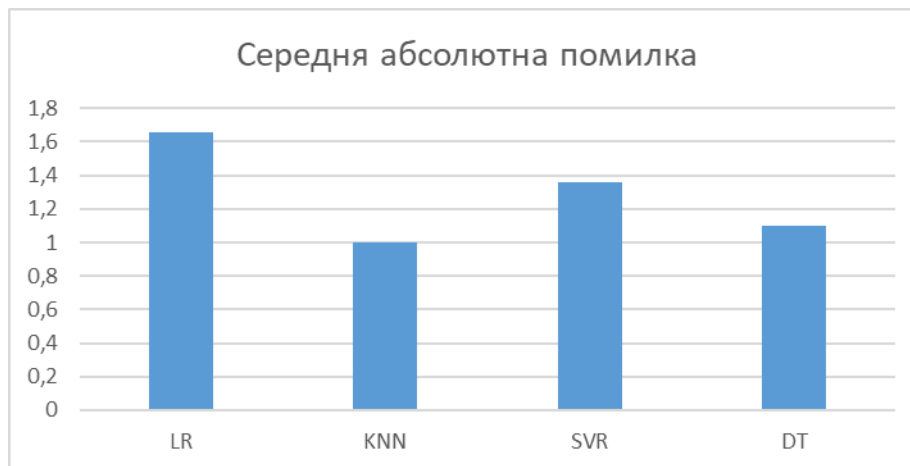


Рис. 3. Середня абсолютна помилка для моделей на основі різних методів машинного навчання.

В моделі на основі методу екстра випадкових дерев відсутні ці негативні фактори, однак і параметри оцінки моделі нижчі. Моделі на основі лінійної регресії та методу к-найближчих сусідів виявились не здатними ефективно прогнозувати оцінку стану людини.

Було досліджено ефективність методів машинного навчання для прогнозування оцінки стану людини, базуючись на отриманих даних від НАНЦ України про зимівників. Дане дослідження дозволить прогнозувати зміну суб'єктивного стану людини на основі проходження тесту кольорової преференції, що дає змогу завчасно реагувати на погіршення психофізіологічного стану людини. В майбутньому планується реалізувати даний підхід у вигляді окремого програмного модулю, з можливістю інтеграції його з ПЗ НАНЦ України. В ПЗ планується використати метод опорних векторів, оскільки при його дослідженні були отримані найкращі параметри оцінки для прогнозування оцінки стану людини.

Література

1. Мадяр А.Й. Инновационные методы исследований в психофизиологии цветового восприятия: Методическое пособие / С.- А. И. Мадяр, Е. В. Моисеенко Е. Э. Ковалевская // – К., 2015. – с. К.
2. Мадяр С.-А.Й. Методика поліхромно-адаптаційної біорегуляції психофізіологічного стану людини (методичні рекомендації) / С.- А. И. Мадяр, Є. В. Моїсеєнко, Г. Ю. Пишнов //– К., 2006.
3. Шитиков В. К. Классификация, регрессия, алгоритмы Data Mining с использованием R./ В. К. Шитиков, С. Э. Мاستицкий // – К., 2017.

АРХІТЕКТУРНЕ РІШЕННЯ ЩОДО СИСТЕМИ АНАЛІЗУ ДАНИХ ОБЧИСЛЮВАЛЬНИХ ПРОЦЕСІВ

Бугаєнко Ю.М., Ляшенко А.В.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: andrey.lyashenko44@gmail.com

ARCHITECTURAL SOLUTION FOR THE SYSTEM OF DATA ANALYSIS OF COMPUTATIONAL PROCESSES

When designing and developing real data analysis systems, a problem arises - high load, due to the large amount of data, on the system. This article explored the effectiveness of a microservice architecture. An architectural solution based on Cloud-computing technologies and micro-services is proposed, which will help to reduce the server load when performing computing processes, in particular, a data analysis system, in which algorithms for cleaning, clustering, building fuzzy logical rules and displaying in the form of a metagraph are performed. The main idea behind this solution was to split the monolithic system into smaller micro-services, each of which is responsible only for its own computational process. As a result, it is possible to use less capacity of each microservice, which will reduce the price, increase the fault tolerance of the system, and these services can be used in the construction of such systems. This architectural solution was tested on the Azure cloud platform as a result of the development of the "Fuzzy Knowledge Base" system for analyzing data on energy efficiency of computing servers. As a result, during the "Performance Testing", a decrease in server load by 37.4% was revealed.

При проектуванні й розробці реальних систем аналізу даних з'являється проблема – високої завантаженості, через великий обсяг даних, на систему. В цій статті проведене дослідження ефективності застосування мікросервісної архітектури. Пропонується архітектурне рішення, яке базується на технологіях Cloud-computing та мікро-сервісів, що допоможе зменшити навантаження сервера під час виконання обчислювальних процесів, зокрема системи аналізу даних, в якій виконуються алгоритми очистки, кластеризації, побудови нечітких логічних правил та відображення у вигляді метаграфа. Головною ідеєю даного рішення було розбиття монолітної системи на менші мікро-сервіси, кожен з яких відповідає тільки за свій обчислювальний процес. В результаті цього можна використовувати меншу потужність кожного мікросервіса, що зменшить ціну, збільшить відмовостійкість системи та ці сервіси можна буде використовувати в побудові схожих систем. Дане архітектурне рішення було опробовано на хмарній платформі Azure, в результаті розробки системи «Fuzzy Knowledge Base», для аналізу даних щодо енергоефективності обчислювальних серверів. В результаті під час «Perfomance Testing», було виявлено зменшення навантаження сервера на 37,4%.

Опис архітектурного рішення. Суть архітектурного рішення полягає в тому, що кожна логічна частина системи повинна бути відокремлена та винесена в окремий мікро-сервіс, який можна легко підключити та інтегрувати до системи, незважаючи на те, яку технологію він використовує в реалізації.

Початкова система мала вигляд моноліту та мала досить багато

недоліків, тобто вся усі функції обробки даних було розроблено в одному проекті та цей проект можливо було розгорнути тільки на одному сервері.

Недоліки монолітної системи:

- Систему можна масштабувати тільки вертикально, тобто збільшуючи обчислювальні характеристики сервера (Процесор, операційну пам'ять)
- Існуючий код програмного забезпечення досить важко підтримувати та модифікувати
- Неможливість використовувати окрему частину системи, як одне ціле при інтеграції в інші систему.
- При досить великому навантаженні та під час завантаження файлів, великої розмірності потрібно збільшувати обчислювальні ресурси сервера, що є досить дорого.

Через вище перелічені недоліки при подальшій розробці системи таке архітектурне рішення було не універсальним, тому було вирішено використати мікро-сервісний підхід.

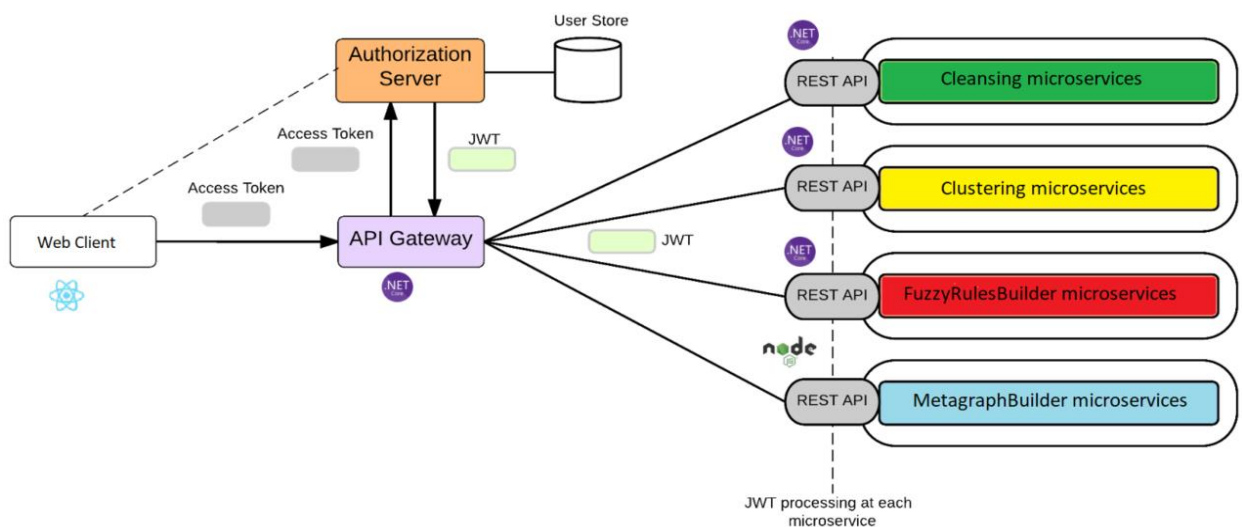


Рис. 1. Архітектура системи на основі мікросервісного підходу.

Кожну частину системи було виділено в окремий проект, який розміщувався на окремому сервері [1]. Система представляє собою веб-сайт, клієнтську частину якого написано на Java-Script із застосуванням бібліотеки React.

Система також має аутентифікацію та авторизацію. Через клієнтську частину під час авторизації клієнт отримує JWT-Token (стандарт токена доступу на основі JSON) від сервера авторизації, за допомогою якого може авторизуватися на кожному із сервісів.

API Gateaway можна назвати головним проектом, яке служить шлюзом

Всі сервіси використовують REST – це архітектурне рішення для взаємодії компонентів розподіленої системи в мережі. Взаємодія між сервісами відбувається через HTTP Requests.

Розглянемо результати. Було проведено дослід на однакових даних, з тією самою кількістю користувачів. При мікросервісній архітектурі навантаження менше на 37,4%.

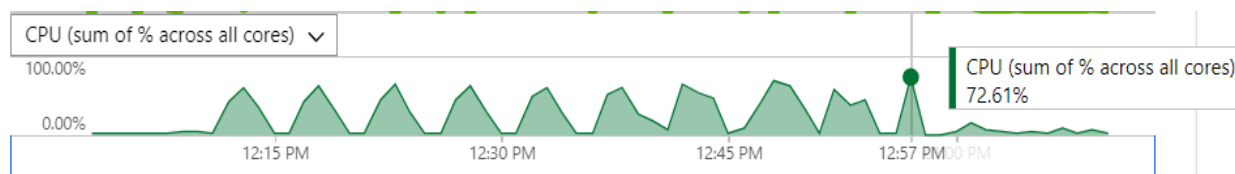


Рис. 3. Навантаження монолітної архітектури.

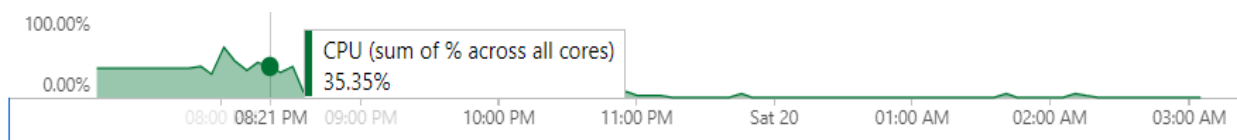


Рис. 4. Навантаження мікросервісної архітектури.

Таким чином, мікросервісна архітектура має перевагу у продуктивності ніж монолітна.

Висновки. В даній статті було запропоноване архітектурне рішення щодо системи аналізу даних обчислювальних процесів, досліджено ефективність мікросервісної архітектури на базі Cloud-computing для його реалізації. Це рішення базується на розбиванні монолітної архітектури на мікросервіси. Кожен сервіс являє собою логічну частину системи, яка може легко інтегруватися з будь-якою системою. Сервіси взаємодіють із головним проектом, який використовується як шлюз, що пересилає запити на відповідний сервіс та агрегує ці дані в одну модель для відображення на клієнтській частині системи, що дозволило зменшити навантаження на систему під час проведення обчислень не менш як на 37,4%.

В майбутньому планується модифікувати дану систему, а саме алгоритми кластеризації та алгоритми очищення даних із статичного набору.

Література

1. <https://docs.microsoft.com/ru-ru/dotnet/architecture/microservices/>
2. 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.
3. Нечеткое моделирование и управление. А. Пегат с. [506-520].

ПРОБЛЕМНІ ПИТАННЯ ПРИ ВИКОРИСТАННІ КОНЦЕПЦІЇ ЛІТ В ПРОМИСЛОВОМУ ВИРОБНИЦТВІ І СПОСОБИ ЇХ ВИРІШЕННЯ

Берлоус В.О., Штогріна О.С.

Інститут телекомунікаційних систем КПП ім. Ігоря Сікорського, Україна

E-mail: McFord@ukr.net

PROBLEM ISSUES WHEN USING THE JIT CONCEPT IN INDUSTRIAL PRODUCTION AND WAYS TO SOLVE THEM

This paper proposes the delivery scheme which combine routes into rings. Reducing the number of return trips with an empty trailer reduce the total batch delivery time to all factories.

В роботі запропонована схема доставок при використанні якої маршрути об'єднуються в кільця. Завдяки наданій схемі буде зменшено кількість зворотних поїздок з пустим причепом та скоротиться загальний час поставок партій на всі заводи.

Сучасні технології транспортних систем, інтернет зв'язку і моніторингу дозволяють за короткий час доставити будь-який товар звідки завгодно будь куди. Швидкими темпами йде процес глобалізації й відновлюються спроби впровадження японського досвіду виробництва на західних підприємствах. Вже успішно впроваджена система Канбан на VAG, GM, Renault, "ЗМЗ", а з вітчизняних виробників – Nissan Motor Ukraine, "Чумак" та "АВК" [1, 2]. Вже зараз є можливість з України дистанційно оформити по індивідуальному замовленню автомобіль концерну VAG, що протягом декількох тижнів буде зібраний і доставлений до українського дилера. Без націнок, так як купівля реалізується через передплату й VAG має гарантію збуту даного автомобіля. Масове виробництво індивідуальних замовлень – ідеологія четвертої промислової революції, що впроваджується на виробництвах головним чином через застосування практики ощадливого виробництва.

Ощадливе виробництво – це система виробництва орієнтована на максимальну гнучкість виробництва під потреби ринку, а її основні заходи спрямовані на усунення витрат на сам перед пов'язаних зі зберіганням та перевиробництвом. В систему ощадливого виробництва входить вище згадана концепція менеджменту Канбан та методологія організації поставок Just In Time (JIT, англ. "Якраз вчасно").

Канбан – концепція менеджменту за якою на кожну сировину та деталь чіпляється RFID (Radio Frequency IDentification) в якому насамперед зберігається інформація про виріб якому вона належить. Кожен двигун суворо закріплений за автомобілем з конкретним VIN-номером. Склад на виробництві виконує не стільки функцію зберігання, скільки точку розподілу - приміщення з великою пропускною здатністю при відносно малій місткості. Запаси зводяться до мінімуму. Їх рівно стільки, щоб була можливість швидко замінити браковану деталь [3]. Відповідно немає потреби доставляти та зберігати сировини більше, ніж це потрібно в даний час. Тобто необхідно доставляти якраз вчасно, чому й присвячена методологія поставок JIT. Середня тривалість перебування сировини на точці розподілу – 6 годин [4].

Зростає залежність від постачальників, зокрема продуктивність заводу починає напряду корегувати з ефективністю системи поставок. Якщо нова партія сировини буде надходити з запізненнями, після того як сировина закінчиться на точках розподілу, то завод буде вимушений тимчасово припинити виробництво. Система ощадливого виробництва принципово уникає практики поставок сировини заздалегідь, бо вона неминуче приводить до перевиробництва. Поставки й виробництво реалізуються виключно за наявності замовлення. Актуальною є задача організації поставок таким чином, щоб найбільше заводів могли працювати одночасно, а кожний окремий транспортний засіб, який доставляє сировину від постачальника до виробника, мав максимальне відношення ваги доставленого вантажу до пройденої дистанції.

Найкоротший та найшвидший спосіб доставити сировину з однієї точки в іншу – завантажити транспортний засіб по максимуму замовленнями з цільової точки та їхати напряду. Однак в масштабі декількох споживачів, зіркова схема розвезень проявляє свою неефективність. Як видно з рисунку 1, щоб задовільнити попит на двох пунктах, транспортний засіб повинен проїхати дистанцію $d_{01} + d_{10} + d_{02} + d_{20}$, половину якої транспортний засіб проїде з пустим причепом [5].

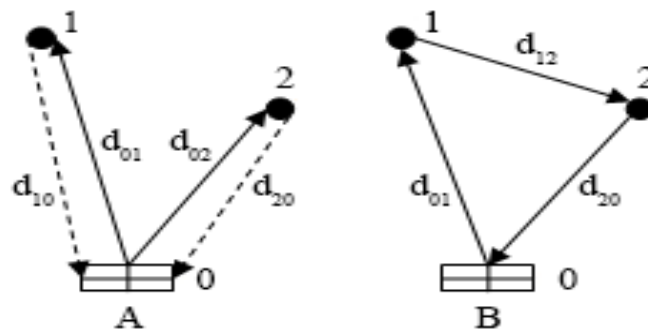


Рис. 1. Схеми поставок:
А – зіркова схема поставок; В – кільцева схема поставок.

Пропонується кільцева схема поставок, при використанні якої маршрути об'єднуються в кільце таким чином, щоб отримати максимальний виграш по дистанції з використанням всього вантажного простору транспортного засобу. По кільцевій схемі, в транспортний засіб завантажуються партії сировини відразу для обох пунктів, які він розвозить послідовно за один маршрут сумарною довжиною в $d_{01} + d_{12} + d_{20}$.

Однак не завжди таке об'єднання буде виправданим й є необхідність в обчислюванні виграшу по дистанції за формулою:

$$S_{ij} = d_{0i} + d_{0j} - d_{ij} ,$$

де S_{ij} – виграш по дистанції; d_{0i} – відстань від бази до пункту i ; d_{0j} – відстань від бази до пункту j ; d_{ij} – відстань між пунктами i та j .

Після чого складається матриця відстаней та виграшів, та знаходиться об'єднання маршрутів на предмет найбільшого виграшу по дистанції S_{max} , що задовольняє наступні умови:

- пункти i та j не входять до одного маршруту;

- пункти i та j є початковими або кінцевими на своїх маршрутах.

Маршрути об'єднуються в кільце доти, поки сумарний попит на пунктах менше вантажопідйомності транспортного засобу. Кільце розширюється на пункт якщо:

- послідовність маршруту до пункту i не змінюється;
- зберігається зв'язність пунктів i та j ;
- послідовність маршруту після пункту j не змінюється.

Якщо сформований кільцевий маршрут не задовольняє весь попит, формується нове кільце.

Отримані кільцеві маршрути з відповідними замовленнями закріплюються за транспортними засобами. Сервіси на зразок Google Maps, уточнюють маршрут, по яким саме дорогам необхідно їхати до заводу з урахуванням поточної дорожньої ситуації (затори, ремонтні роботи і т.д.) [6] й власне реалізується доставка партій.

Запропонована схема оперує мало партійними доставками – в транспортний засіб завантажуються штучні партії з декількох заводів, а не одне велике замовлення з одного заводу. По завершенню маршруту поставок, завод буде мати менший запас сировини у порівнянні з зірковою схемою, однак одночасно зможуть працювати більше заводів. Середній час поповнення заводів загалом зменшується за рахунок зведення до мінімуму зворотних поїздок з пустим причепом, а також охоплення маршрутом декількох точок. Таким чином охоплюється більший попит й відповідно зменшується час очікування накопичень замовлень на обраний маршрут. Скоріше можна відправляти транспортний засіб по маршруту доставки. Партії швидко закінчуються але й швидко поповнюються, що відповідає концепції JIT.

Література

1. «Об эффективности модели работы фирмы «Тойота». Реалии современного мирового автомобилестроения». URL: <http://www.avtomash.ru/guravto/2005/20051137.htm> (дата звертання: 16.02.2021).
2. Вольвач І. Ю. Досвід Впровадження Логістичної Концепції Виробництва “Just-in-time”. Економічні науки. URL: http://journals.khnu.km.ua/vestnik/pdf/ekon/2009_4_2/pdf/250-253.pdf (16.02.2021).
3. «Что такое система Канбан и в чем ее основной смысл». URL: <https://rdv-it.ru/company/press-center/blog/sistema-proizvodstva-kanban/> (дата звертання: 16.02.2021).
4. «Внедрение системы точно в срок на примере. Быть вовремя во всем Just-In-Time (JIT)». URL: <https://avtopilot-center.ru/vnedrenie-sistemy-tochno-v-srok-na-primere-byt-vovremya-vo.html> (дата звертання: 29.12.2020).
5. «Метод Кларка-Райта. Оптимальное планирование маршрутов грузоперевозок». URL: <https://infostart.ru/1c/articles/443585/> (дата звертання: 23.10.2020).
6. Никоноров В.М. Усовершенствование метода Кларка-Райта для решения задачи автомобильных мелкопартийных перевозок. Киберленинка. Экономико-математические методы и модели. URL: <https://cyberleninka.ru/article/n/usovershenstvovanie-metoda-klarka-rayta-dlya-resheniya-zadachi-marshrutizatsii-avtomobilnyh-melkopartionnyh-perevozok/viewer> (дата звертання: 09.02.2021).

ЗАСТОСУВАННЯ ОНТОЛОГІЙ В ТЕЛЕКОМУНІКАЦІЯХ

Ладичук О.К., Попова М.А.

Національний центр «Мала академія наук України», Україна

E-mail: sasha.ladychuk@gmail.com, pm@man.gov.ua

ONTOLOGIES APPLICATION IN TELECOMMUNICATIONS

Ontology, as semantic interoperability and knowledge sharing foundation, is increasingly used in the telecommunications domain, consisting of a large number of concepts and relationships between them. To solve the problem of Big Data, different ontologies compatibility and the formation of the telecom company business processes unified ontological environment it is proposed to use CIT "POLYHEDRON" to create ontologies of telecommunications services to support knowledge sharing and reuse.

Сучасна епоха становлення економіки знань вимагає формування проактивного індивіда – нової генерації критично мислячих, науково грамотних, творчих людей, здатних нестандартно вирішувати комплексні завдання. Будь-яка діяльність в економіці знань вимагає високого рівня володіння інформаційними технологіями та інноваційного мислення. В Україні осередком підготовки майбутніх абітурієнтів, які володіють не лише знаннями з основ наук, але й дослідницькими та винахідницькими навичками, є Національний центр «Мала академія наук», науковці якого розробляють засоби та технології підтримки науково-освітньої діяльності учнівської молоді, зокрема в галузі інформаційно-телекомунікаційних технологій.

Так, наприклад, для вирішення проблеми великих даних (Big Data) в галузі телекомунікаційних послуг, що призвела до зростання складності та неоднорідності сучасної мережевої інфраструктури внаслідок існування безлічі операторів та постачальників обладнання для телекомунікаційних мереж, кожен з яких розробляє та будує свої власні механізми та власні версії конфігурації, опис документів, технічні специфікації та програмні системи для пристроїв із подібною функціональністю, пропонується використання комп'ютерних онтологій [1].

За останні десятиліття практика застосування онтологій в телекомунікаціях набула широкого поширення. Наприклад, онтологія домену телекомунікаційних послуг (Telecommunications Service Domain Ontology, TSDO) охоплює питання семантичної взаємодії телекомунікаційних послуг, утворюючи спільні словники для підтримки веб-додатків з метою семантичного опису телекомунікаційних послуг, виявлення послуг та моделювання їх контексту [2]. Завдяки великій кількості описаних термінів/понять (430 концептів та 245 властивостей) і технологій, що зустрічаються в галузі телекомунікаційних послуг, мережа виступає сховищем знань та засобом моделювання бізнес-процесів організації [3].

TOUCAN Ontology (ToCo) [4] здатна описати фізичну інфраструктуру гібридних телекомунікаційних мереж, включаючи пристрої, інтерфейси та технології відношення в мережах усіх доменів в сучасній телекомунікаційній

системі. До того ж, до переліку концептів ToCo (84 концепти, 39 властивостей об'єктів та 54 властивості типів даних) включені як послуги, що надаються телекомунікаційними мережами, так і користувачі, які обслуговуються, оскільки є частиною телекомунікаційної системи. Завдяки цій онтології також може бути оцінена якість послуг зв'язку, наприклад, пропускна здатність, швидкість передачі даних, втрата пакетів, затримка тощо.

Метою онтології OntoGate [5] є оцінка та відбір ідей в процесі інноваційної діяльності телекомунікаційної компанії, а онтології IdeaOntology [6] - забезпечення спільної мови для поширення ідей з використанням зважених оцінки та засобів представлення результатів.

Отже, досвід застосування онтологій для менеджменту даних, забезпечення їх семантичної взаємодії та надання додаткових сервісів з оцінки, аналізу та вибору послуг телеком-компанії досить багатий. Проте на сьогоднішній день різноманітність таких онтологій вимагає зусиль із забезпечення узгодження між ними шляхом стандартизації описаних даних для формування бізнес-процесу повного циклу компанії, і окремі телекомунікаційні суб'єкти все ще стикаються з проблемами при інтеграції власних даних: від синтаксичних відмінностей (наприклад, від різних термінологій, стандартів і форматів) до більш глибоких семантичних відмінностей (наприклад, різної деталізації для етапів моделювання бізнес-процесу).

Тому на практиці необхідно не лише об'єднати декілька онтологій, щоб повністю реалізувати змістовну інтеграцію та аналіз даних у галузі телекомунікацій, а й розробити рішення, які можуть автоматизувати цей процес або мінімізувати зусилля людини, забезпечуючи семантичну взаємодію.

Одним з таких рішень є застосування когнітивних ІТ-технологій, що забезпечують процес семантичного аналізу інформаційних ресурсів незалежно від формату, стандартів та технологій їх створення. Когнітивні сервіси здатні реалізувати структурування і класифікацію інформації, синтезувати необхідні документи на основі семантичного аналізу, виявити властивості інформаційних процесів й забезпечити вибір та прийняття оптимальних рішень для прогнозування їх розвитку [7]. Фактично когнітивні ІТ-технології спроможні реалізувати повномасштабну інтеграцію інформаційних ресурсів, утворюючи єдиний інформаційний простір. Такий підхід може забезпечити доступ до відповідної інформації кожному суб'єкту телекомунікаційної галузі згідно його функціональних завдань та посадових обов'язків, а також створити технологічні умови налагоджування ефективної взаємодії між телеком-компаніями.

Для реалізації онтологій, зокрема в галузі телекомунікацій, в процесі навчально-дослідницької діяльності учнівської молоді науковцями НЦ «МАНУ» пропонується когнітивна інформаційна технологія (KIT) «ПОЛІЕДР» [8], призначена для підтримки процесів семантико-лінгвістичного аналізу великих обсягів просторово-розподіленої неструктурованої інформації (Big Data), їх структурування, встановлення контекстних зв'язків між документами, що обробляються, прогнозування та підтримки процесів раціонального вибору з наступним формуванням інформаційно-аналітичних веб-орієнтованих рішень.

КІТ «ПОЛІЕДР» забезпечує опрацювання великих даних та підтримку форматів і протоколів W3; семантико-лінгвістичний аналіз різноформатних інформаційних ресурсів, які мають значну кількість міждисциплінарних відношень та створені на основі використання різних інформаційних технологій і стандартів; трансдисциплінарний аналіз та інтеграцію з іншими мережевими інформаційними системами та веб-орієнтованими додатками; таксономічне (ієрархічне) відображення структури інформаційних масивів, включаючи міжконтекстні зв'язки; створення онтологічних інтерактивних документів; виявлення латентної інформації в аналізованих інформаційних ресурсах; синхронізацію документації, отриманої з різних джерел; індексне маркування інформаційних масивів; формування та відображення динамічних тематичних класифікаторів, каталогів та реєстрів інформаційних ресурсів; виявлення синонімічної еквівалентності між інформаційними масивами, що відображаються українською та англійською мовами; прогнозне оцінювання; підтримка процесу прийняття рішень на основі таксономічного представлення структури інформаційних масивів, що аналізуються; формування інформаційних документів (довідок, звітів, запитів тощо).

Таким чином, онтологія як базис семантичної взаємодії та обміну знаннями все частіше застосовується в галузі телекомунікацій, що складається з великої кількості понять і відношень між ними. Для вирішення проблеми великих даних, сумісності різних онтологій та формування єдиного онтологічного середовища бізнес-процесів телеком-компанії пропонується використання КІТ «ПОЛІЕДР» з метою створення онтологій телекомунікаційних послуг для підтримки обміну знаннями та їх повторного використання.

Література

1. Globa L.S., Popova M.A., Yushko N.A. Improved Approach to Quality Control of Telecommunication Service Providers. *Proceedings of International Conference on Applied Innovation in IT (ICAIIIT)*, 2020, 8(1), Pp. 29–34.
2. Qiao, X., Li, X., Chen J. Telecommunications Service Domain Ontology: Semantic Interoperation Foundation of Intelligent Integrated Services. *Telecommunications Networks - Current Status and Future Trends*. IntechOpen. 2012. P.183-210
3. Ford, A. Fox, M.S. A Telecommunications and Innovation Ontology for Global City Indicators (ISO 37120). *GCI Telecommunications and Innovation Ontology*. 2015. Pp-1-35.
4. Zhou Q., Gray A.J.G., McLaughlin S. ToCo: An Ontology for Representing Hybrid Telecommunication Networks. Hitzler P. *The Semantic Web. ESWC 2019. Lecture Notes in Computer Science, vol 11503*. Springer, Cham, 2019.
5. Burlinger, A.S. Innovation and Ontologies. Gabler/ GWV Fachverlage, 2008. 409 p.
6. Riedl, C., May, N., Finzen, J., Stathel, S., Kaufman, V., Krcmar, H. An Idea Ontology for Innovation Management. *International Journal on Semantic Web and Information Systems (IJSWIS)*, 2009. Vol. 5, № 4. P. 1-18.
7. Dovgyi S., Stryzhak O. (2021) Transdisciplinary Fundamentals of Information-Analytical Activity. In: Ilchenko M., Uryvsky L., Globa L. (eds) *Advances in Information and Communication Technology and Systems*. MCT 2019. Lecture Notes in Networks and Systems, vol 152, Pp. 99-126. Springer, Cham.
8. Свідоцтво про авторське право на твір №96078 від 17.02.2020 р. “Комп’ютерна програма “Когнітивна ІТ платформа ПОЛІЕДР” (“КІТ ПОЛІЕДР”) (“POLYHEDRON”) Автори. Стрижак О.В., Глоба Л.С., Величко В.Ю., Попова М. А. та ін. Офіційний бюлетень №57 (31.03.2020) с. 402-403.

**АЛГОРИТМИ УКРУПНЕННЯ СТАНІВ
МЕРЕЖІ ПЕРЕДАЧІ ДАНИХ В ЗАДАЧАХ
ОЦІНКИ МЕРЕЖЕВИХ ХАРАКТЕРИСТИК**

Зайченко Ю.П., Васильєв В.І., Віштал Д.М., Любашенко Н.Д.

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

E-mail: d.vishtal@kpi.ua

**ALGORITHMS OF INTEGRATION OF STATUS
CONDITIONS IN DATA COMMUNICATIONS NETWORK IN PROBLEM
OF ESTIMATION OF NETWORK CHARACTERISTICS**

Algorithms of structural (topological) integration of statuses of system depending on formulary representation of monotonous structural function of availability of network service in the form of minimal disjunctive normal form - MDNF (minimal conjunctive normal form - MCNF) in class of binary stochastic models are considered.

В залежності від задач, розв'язуваних користувачами мережі передачі даних (МПД), до мережі пред'являються вимоги по структурній і (або) функціональній надійності мережевої послуги. Характеристики структурної (топологічної) надійності відображають можливість мережі надавати зв'язок абонентам у довільний проміжок часу. Характеристики функціональної надійності відображають можливості мережі надавати абонентам зв'язок у проміжку заданого інтервалу часу. До функціональних характеристик також відноситься середній стаціонарний час перебування мережі в підмножині станів доступності (недоступності) мережевої послуги відповідно до заданої структурної функції.

Доступність мережевої послуги є універсальною характеристикою, використовуваною як постачальниками послуг так і користувачами.

В якості статичної моделі мережі розглядається розмічений кінцевий зв'язний граф $G(Y;X)$ без петель, де $|Y|$ - число вузлів графа, $|X|$ - число ребер графа. Вузли графа відіграють допоміжну роль. Матриця суміжності вузлів графа використовується для знаходження представлення детермінованих графових властивостей відповідними структурними функціями.

В якості динамічної моделі мережі розглядається стохастичний граф, елементи якого зважені ваговими параметрами. Простір станів стохастичного графа W_G можна розглядати і як векторний простір по mod (2) [1] і як булеву векторну решітку B_2^n . Використання простору W_G зручно для алгоритму знаходження розрізаючих множин графа, циклів та остовів. Векторний простір W_G містить два ортогональних підпростори циклів і розрізів,

розмірність яких дорівнює відповідно цикломатичному числу й рангу графа. Мережа призначена для забезпечення мережевої послуги в будь-який момент часу для всіх пар вузлів. Довільна пара вузлів може одержати мережеву послугу, якщо в цей момент часу знайдеться принаймні один простий шлях, їх з'єднуючий. Мережева послуга доступна для всіх вузлів, якщо в цей момент часу існує принаймні одне остовне дерево.

Елементи мережі й структурні функції, що відповідають умовам доступності мережевої послуги, приймають бінарні значення. Нехай $\varphi(x_1(t) \dots x_n(t)) = \varphi(t)$ - детермінована структурна функція випадкових величин, що відповідає деякому виду мережевої послуги. Випадкова величина $x_i(t)$ ($i=1, \dots, n$) дорівнює 1, якщо в момент t i -й елемент доступний для виконання мережевої послуги й дорівнює 0 – у протилежному випадку. Функція $\varphi(t)$ дорівнює 1, якщо в момент t мережева послуга здійсненна й 0 - у протилежному випадку. Аксиоми булевої алгебри погоджені із законами інтуїтивної логіки для множин, висловлювань, предикатів і властивостей.

Ізоморфізм булевої алгебри класів і відповідної булевої алгебри властивостей дає можливість алгебраїзації необхідних обчислень для оцінки характеристик доступності мережевої послуги. Функціонування мережі розглядається як процес випадкового блукання по булевій векторній решітці

Прийняті допущення бінарної стохастичної моделі:

1. Статистичною залежністю на рівні окремих елементів можна зневажити.

2. Еволюція елементів моделюється в часі відповідними альтернуючими процесами відновлення з кінцевими середніми значеннями інтервалів доступності (недоступності) для виконання мережевої послуги [2].

3. Вектор стану елементів однозначно визначає стан доступності (недоступності) мережевої послуги.

4. Існує $\lim_{t \rightarrow \infty} P\{x_i(t) = 1\} = \frac{M\theta_i}{M\theta_i + M\xi_i} = P_i$, де $M\theta_i$, $M\xi_i$ - середні стаціонарні інтервали доступності (недоступності) i -го елемента для виконання мережевої послуги.

5. Простір станів елементів розглядається як булева векторна решітка [3].

6. В якості критеріального простору мережі розглядається множина всіх ізотонних відображень булевої векторної решітки B_2^n у множину B_2 [3].

Умови незалежності функціонування елементів й існування ймовірностей $P_i, i=1, \dots, n$ визначають існування й однозначність ймовірнісної міри на булевій алгебрі всіх підмножин булевої векторної решітки.

В цих умовах потрібно оцінити точно або приблизно наступні мережеві

характеристики:

$h_{\varphi} (P_1, \dots, P_n)$ – стаціонарна ймовірність доступності мережевої послуги;

$M_{\theta_{\varphi}}, M_{\xi_{\varphi}}$ – середні стаціонарні інтервали доступності (недоступності)

мережевої послуги.

Основна обчислювальна проблема оцінки мережевих характеристик обумовлена складністю структурної організації мережі й великою розмірністю простору станів. Ця обставина обумовлює важкість обчислення мережевих характеристик. Можна на декілька порядків підняти поріг точної обчислювальності мережевих характеристик, використовуючи декомпозицію структурної функції, властивість дуальних автоморфізмів булевої алгебри та алгоритми представлення структурної функції в ортогональній неповторній формі. Декомпозиція структурної функції дозволяє здійснити структурно-фазове укрупнення станів мережі [4,5].

Детерміновані властивості монотонних структурних функцій однозначно визначаються наступними МДНФ (МКНФ)-формульними тотожностями:

$$\bigvee_{\{\alpha_i\} \in I} \left(\bigwedge_{k_i \in \{\alpha_i\}} x k_i \right) = \varphi(x_1, \dots, x_n) = \bigwedge_{\{\beta_j\} \in J} \left(\bigvee_{r_j \in \{\beta_j\}} x r_j \right) \quad (1)$$

$$\bigvee_{\{\beta_j\} \in J} \left(\bigwedge_{r_j \in \{\beta_j\}} x r_j \right) = \varphi^*(x_1, \dots, x_n) = \bigwedge_{\{\alpha_i\} \in I} \left(\bigvee_{k_i \in \{\alpha_i\}} x k_i \right) \quad (2)$$

$$\bigvee_{\{\beta_j\} \in J} \left(\bigwedge_{r_j \in \{\beta_j\}} \overline{x} r_j \right) = \overline{\varphi}(x_1, \dots, x_n) = \bigwedge_{\{\alpha_i\} \in I} \left(\bigvee_{k_i \in \{\alpha_i\}} \overline{x} k_i \right) \quad (3)$$

$$\bigvee_{\{\alpha_i\} \in I} \left(\bigwedge_{k_i \in \{\alpha_i\}} \overline{x} k_i \right) = \overline{\varphi}^*(x_1, \dots, x_n) = \bigwedge_{\{\beta_j\} \in J} \left(\bigvee_{r_j \in \{\beta_j\}} \overline{x} r_j \right) \quad (4)$$

де $\bigwedge_{k_i \in \{\alpha_i\}} x k_i = \alpha_i(x)$ – і-та проста імпліканта функції $\varphi(x)$,

$\{\alpha_i\}$ – набір індексів істотних змінних і-ої імпліканти,

$\bigwedge_{r_j \in \{\beta_j\}} x r_j = \beta_j(x)$ – j-та проста імпліканта двоїстої функції $\varphi^*(x)$,

$\{\beta_j\}$ – набір індексів істотних змінних j-ої імпліканти,

$\bigvee_{k_i \in \{\alpha_i\}} x k_i = \alpha_i^*(x)$ – двоїста стосовно $\alpha_i(x)$ функція,

$\bigvee_{r_j \in \{\beta_j\}} x r_j = \beta_j^*(x)$ – двоїста стосовно $\beta_j(x)$ функція.

Інтерпретація інших компонентів тотожностей визначається аналогічно.

Символ I використовується як для позначення повного списку простих імплікант функції $\varphi(x)$ так і для позначення індексів сімейств істотних

змінних простих імплікант. Символ J використовується аналогічним чином.

Зробимо декілька зауважень:

1. Тотожності (1-4) дають можливість знаходити мінімальне по кількості літералів МДНФ (МКНФ)-представлення відповідних структурних функцій. Однак при цьому втрачається незалежність функціонування, розглянута на рівні простих імплікант функцій. У загальному випадку прості імпліканти не є незалежними випадковими величинами.
2. Тотожності (1-4) вірні не тільки для бінарних значень змінних, але й для безперервних не негативних значень змінних. З комбінаторної точки зору теоретико-множинні сімейства індексів простих імплікант

$$I = \left\{ \left\{ \alpha_i \right\} \right\}_{i=1}^{|I|} \text{ та } J = \left\{ \left\{ \beta_j \right\} \right\}_{j=1}^{|J|}$$

утворюють два двоїстих сімейства мінімальних трансверсалей.

3. Знання M_{θ_i} , M_{ξ_i} а також сімейств множин I та (або) J дає можливість виявляти “вузькі місця” у забезпеченні мережових характеристик, визначати ступінь впливу на ці характеристики як окремих елементів так і певних конфігурацій елементів, що важливо для мереж, які розвиваються або проектуються.

Висновки. Для оцінки характеристик мережі використовуються ефективні алгоритми пошуку сімейств I та J, а також алгоритми декомпозиції структурної функції. З цією метою використовується покрокове розкладання Шеннона з урахуванням поглинання до одержання неповторної ортогональної форми й, при необхідності, узагальнені формули Де Моргана. В роботі розглядаються ілюстративні приклади оцінки мережових характеристик в залежності від вагових параметрів елементів та різних структурних функцій.

Література

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.

ПРОЕКТУВАННЯ МУЛЬТИСЕРВІСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ВІДОМЧОГО ПРИЗНАЧЕННЯ НА ОСНОВІ БАГАТОКРИТЕРІАЛЬНОГО ПІДХОДУ

²Вакулєнко О.В., ²Дорошенко А.С., ¹Луцький А.О.

¹Інститут спеціального зв'язку та захисту інформації КПІ ім. Ігоря Сікорського

²Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: morgot141@gmail.com

REVEALS THE GENERAL APPROACHES OF DESIGNING STAGES OF MULTISERVICE NETWORKS OF SPECIAL PURPOSE

Reveals general approaches of designing multiservice telecommunication networks for departmental purposes based on a multi-criteria approach.

Проектування мультисервісних телекомунікаційних мереж відомчого призначення – це процес розробки системно-технічних рішень по їх побудові при короткостроковому, середньостроковому і перспективному розвитку (плануванні). Процес проектування є складною науково-технічною задачею, яка ґрунтується на використанні результатів теорії систем, графів, ефективності, масового обслуговування, математичного програмування і передбачає вирішення комплексу взаємопов'язаних завдань.

При проектуванні мереж зв'язку різного призначення формулюється оптимізаційна задача, яка на основі має наступний вигляд:

$$\Phi = \Phi(W, U) \xrightarrow{extr} \limits_{W \in \Omega_W} \rightarrow W_U^o \quad (1)$$

де Ω_W – допустима безліч, в рамках якої може варіюватися досліджувана мультисервісна телекомунікаційна мережа відомчого призначення;

W_U^o – оптимальна в умовах U мультисервісна телекомунікаційна мережа відомчого призначення (в якості умов функціонування розглядається навантаження, що надходить в мережу, навмисні і ненавмисні зовнішні і внутрішні впливи, що характеризуються властивостями стійкості (надійності, живучості), безпеки зв'язку та ін.).

При вирішенні подібних завдань, як правило, використовуються два методи:

1) Пошук компромісних (ефективних) рішень, оптимальних за Парето (за всіма компонентами векторного критерію);

2) Пошук рішень оптимальних в сенсі узагальненого скалярного критерію, отриманого шляхом згортки окремих компонент векторного критерію.

З урахуванням аналізу розвитку мультисервісних телекомунікаційних мереж відомчого призначення (МТМВП) допускається природна декомпозиція – параметрична і структурна, яка передбачає поетапний (ітераційний) синтез структури та вибір значень внутрішніх параметрів $x_1^{(o)}, \dots, x_n^{(o)}$ (параметрична оптимізація), при яких виконуються вимоги до якості функціонування і вартості проекту:

$$\Phi = \Phi(X, G, U) \xrightarrow{extr} \limits_{G \in \Omega_G} \xrightarrow{extr} \limits_{X \in \Omega_X} \rightarrow G_U^o, X_U^o = [x_1^{(o)}, \dots, x_n^{(o)}]^T, \quad (2)$$

де Ω_X – безліч допустимих параметрів мультисервісної телекомунікаційної мережі

відомчого призначення (пропускна здатність каналів передачі, пріоритети в обслуговуванні, продуктивність обладнання, стійкість мережі та ін.); Ω_G – безліч допустимих структур мультисервісної телекомунікаційної мережі відомчого призначення; X_U^o – оптимальні в умовах U параметри мультисервісної телекомунікаційної мережі відомчого призначення; G_U^o – оптимальна в умовах U структура (граф) мультисервісної телекомунікаційної мережі відомчого призначення.

При цьому вимоги до якості функціонування задаються у вигляді обмежень на вихідні параметри:

$$\alpha_j \leq \gamma_j(X, U) \leq \beta_j, j = \overline{1, n}. \quad (3)$$

де $\gamma_j(X, U)$ – j -й вихідний параметр, який є функцією внутрішніх;

$X = [x_1^{(o)}, \dots, x_n^{(o)}]^T$ і зовнішніх $U = [u_1^{(o)}, \dots, u_n^{(o)}]^T$ параметрів;

α_j, β_j – допустимі межі зміни j -го параметра, що визначаються технічним завданням (ТЗ).

На практиці, як правило, оптимізаційна задача (3) зводиться до знаходження мінімуму функціоналу техніко-експлуатаційних витрат C , що включає вартість оренди каналів передачі $\delta \cdot V$ і наведену вартість поставленого обладнання мережі K (капітальні витрати): $C = \delta \cdot V + K \rightarrow \min_{G \in \Omega_G, X \in \Omega_X} \rightarrow G_U^o, V_U^o$, (4)

при забезпеченні заданих (або досяжних – в умовах обмежень $C \leq C_{max}$) вимог до якості функціонування (визначається на основі спільної ймовірності виконання вимог до якості обслуговування повідомлень різних класів якості $r = \overline{1, R}$, включаючи підсистеми управління, інформаційної безпеки та стійкості мультисервісної телекомунікаційної мережі відомчого призначення, що і визначає багатокритеріальність завдання.

Тут $V \subset X$ – вектор пропускних спроможностей елементів мережі зв'язку, які обирають з номінального ряду швидкостей цифрових систем передачі, $\{V \times 64 \text{кбит/с}, V \times 2048 \text{кбит/с}, \dots, V \times 155 \text{Мбит/с}\}, V = 1, 2 \dots$; δ – питомі витрати на оренду каналів передачі (дискретна величина), які залежать від протяжності маршруту доставки інформації, часу функціонування, а також визначаються чинними тарифами.

Таким чином, наявність важко формалізованих обмежень, багатокритеріальний характер завдання (4) зумовлюють застосування ітераційного алгоритму проектування. Відповідно до цього пропонується метод проектування мультисервісної телекомунікаційної мережі відомчого призначення, що складається з двох взаємопов'язаних етапів.

Перший етап призначений для обґрунтування характеристик застосовуваного телекомунікаційного обладнання, аналізу (формування) топологічної структури мережі, розрахунку (оптимізації) її пропускної здатності і показників якості обслуговування (за класами якості) в стаціонарних умовах функціонування. При цьому для розрахунків передбачається використання процедур статичної маршрутизації і розподілу потоків, а також моделей найпростіших потоків. Останнє обумовлено тривалим інтервалом передбачуваного часу функціонування проекрованої мережі та підтверджується граничною теоремою про збіжність до найпростішого суперпозиції незалежних ординарних стаціонарних (нестационарних) потоків з різною післядією.

Другий етап передбачає більш глибоке дослідження питань забезпечення

(підтримки) якості обслуговування в мультисервісній телекомунікаційній мережі відомчого призначення в умовах самоподібності трафіку вузькосмугових і широкосмугових служб. На даному етапі передбачається розробка методу, що включає (для відповідних умов самоподібності трафіку елементів мультисервісної телекомунікаційної мережі відомчого призначення або мультисервісної телекомунікаційної мережі відомчого призначення в цілому):

а) моделювання процесів формування самоподібного (мультисервісного) трафіку і його обслуговування при різних способах управління (пріоритетне обслуговування, резервування ресурсів та ін.);

б) розрахунок показників якості функціонування СМО з самоподібним трафіком, а також уточнення обсягів накопичувачів і продуктивності вузлів комутації з урахуванням введення класів якості обслуговування.

Висновок:

Багатокритеріальний метод проектування мультисервісної телекомунікаційної мережі відомчого призначення дозволяє:

- досліджувати ефективність процесів функціонування мультисервісної телекомунікаційної мережі відомчого призначення різного призначення в різних умовах застосування на основі узагальнених показників, в тому числі в умовах самоподібності трафіку;
- досліджувати ефективність процесів надання та інтеграції різних видів послуг з різними вимогами до якості обслуговування, з урахуванням функціонування підсистем (управління, інформаційної безпеки);
- здійснювати оптимізацію побудови мультисервісної телекомунікаційної мережі відомчого призначення за критеріями техніко-експлуатаційних витрат, якості обслуговування (з урахуванням введення класів якості обслуговування), стійкості.

В цілому дані фактори визначають новий спосіб побудови структури проектування мультисервісної телекомунікаційної мережі відомчого призначення та взаємозв'язок окремих дослідницьких завдань, що дозволить приймати правильні управлінські рішення щодо вибору раціонального сценарію побудови даних мереж.

Література

1. Алексеев Е.Б., Гордиенко В.Н., Крухмалёв В.В., Моченов А.Д., Тверецкий М.С. Проектирование и техническая эксплуатация цифровых телекоммуникационных систем и сетей. Учебное пособие для вузов. – М.: Горячая линия–Телеком, 2008. – 392 с.
2. Воробієнко П.П., Л.А. Нікітюк Л.А., П.І. Резніченко П.І. «Телекомунікаційні та інформаційні мережі». – 2010.
3. Заїка В.Ф., Варфоломєєва О.Г., Домрачева К.О., Гринкевич Г.О.. «Телекомунікаційні системи та мережі наступного покоління». – 2019.
4. Нікітюк Л.А., Тихонов В.І., Боярських П.В.. «Проектування мультисервісної мережі: методичні вказівки для виконання курсового проекту. Модуль 2. Принципи функціонування мережі. Частина 2». – 2010. – 60 с.
5. Стеклов В.К., Беркман Л.Н., Кільчицький Є.В. Оптимізація та моделювання пристроїв і систем зв'язку: Підруч. для вищ. навч. закл.. – К.: Техніка, 2004. – 576 с.
6. Стеклов В.К., Беркман Проектування телекомунікаційних мереж: Підруч. для вищ. навч. закл. за напрямком «Телекомунікації». – К.: Техніка, 2002. – 792 с.
7. Тарбасв С. І. Проектування інфокомунікаційних мереж. Навчальний посібник. Підготовлений для самостійної роботи студентів вищих навчальних закладів з кредитномодульною організацією навчального процесу. – К: ННІТІ ДУТ, 2015. – 151 с.

ОЧИЩЕННЯ ДАНИХ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ОБРОБКИ ДАНИХ В МЕРЕЖАХ ІОТ

Гребініченко М.В.

Інститут телекомунікаційних систем КІП ім. Ігоря Сікорського, Україна

Email: grebinichenko.maria@gmail.com

DATA CLEANSING FOR INCREASING PERFORMANCE IN IOT NETWORKS

In this article is studying problem of preprocessing big amount of data in IoT networks. One of the methods for resolving this problem is developing new data cleansing dynamic algorithm. The benefits of application of this method are presented and described.

У даній статті розглядається проблема попередньої обробки великих даних у мережах ІоТ. Один з методів вирішення даної задачі - розробка нового динамічного алгоритму очищення даних. Переваги застосування даного методу також представлені.

Зі стрімким поширенням застосування розумних систем Internet Of Things, зросла і кількість інформації, що підлягає обробці на сервері, а також і кількість факторів, що можуть вносити похибки до датасетів або призводити до часткової втрати даних. Тому з'явилася необхідність підвищення достовірності кінцевого результату роботи мережі ІоТ за рахунок очищення даних від випадково виникаючих помилок.

На вхідні дані, які пізніше піддаються обробці та аналізу, впливають ряд різноманітних чинників, як збирання та формування набору з різних джерел, передача їх через світову мережу, умови збору інформації з датчиків (температурний, механічний впливи), програмний збій та безліч інших. Кожен з цих факторів потенційно знижує якість даних, що підлягають обробці. Як наслідок у кінцевих обрахунках можуть виникати невалідні та хибні значення, що практично унеможлиблює отримання корисних результатів із наборів великих даних.

Існує ряд алгоритмів та методів, що розв'язують означену проблему, проте вони не є максимально ефективними, чи розв'язують проблему очищення даних частково. Необхідна модифікація алгоритму попередньої обробки даних для забезпечення гарантовано більш точного результату із мінімальним застосуванням часових та розрахункових ресурсів.

Головною ідеєю виконаного дослідження є визначення такого алгоритму очищення даних, що дозволив би гарантовано підвищити достовірність кінцевого результату обробки даних із максимальною ефективністю.

Проте не всі дані можуть бути зібрані з різних джерел, а отже містити різні структури моделей та мати різні зв'язки між параметрами, або містити пропущені дані, бо датчики збору інформації відпрацювали високоякісно протягом всього періоду роботи. Для кожного окремого випадку та кожного набору даних, що йде на обробку, має бути встановлений відповідний процес очистки.



Рис. 1. Блок-схема модифікованого процесу очистки даних.

Запропонований додатковий блок обробки даних має на меті проаналізувати вхідний датасет та адаптивно створити унікальний порядок дій щодо очистки. Для вибору алгоритмів для обробки мають бути сформовані чіткі критерії вибору. Таким чином вдасться розробити алгоритм, що динамічно буде здатний скласти порядок та складові обробки, і тим самим не лише провести ефективну очистку даних, а й знизити навантаження на систему та кількість часових та програмних ресурсів.

Таблиця 1. Компоненти для динамічної попередньої обробки даних.

Компонент очищення	Тип даних	Короткий опис роботи	Умови автоматичного запуску
<i>Фільтрування даних</i>	Числовий	Видалення нерелевантних пікових значень. Після утворення схеми об'єкту даних, користувачу пропонується для кожного ввести максимальне та мінімальне значення.	Відсоток записів, що не є релевантними за початковими умовами більший за Z_0
<i>Відновлення пропущених значень</i>	Числовий	Заповнення відсутніх значень параметрів у наборах даних. Змінна заповнюється відповідним середнім для параметра значенням.	Відсоток пропущених записів, що не можуть набувати значення NULL більший за Z_0
<i>Видалення дублікатів</i>	Числовий, строковий	Визначення повторюваних записів у датасеті	• Якщо дублікати за певним параметром заборонені, відбуватиметься пошук та їх видалення. Також це стосується наявності дублікатів-об'єктів загалом, або повторюваних записів • Перевірка дублікатів за первинним ключем (якщо у метаданих він наданий). Спершу перевіряються дані за зазначеними полями у ключі, а потім – усі записи без них, тобто, якщо ми вилучимо параметри ключа, чи не буде у записах повністю ідентичних даних.
<i>Приведення текстових значень</i>	Строковий	Текстові поля можуть приймати три класи А Б і В, для кожного рядка в датасеті це один з трьох даної колонки (А, Б, В) На виході отримуємо 3 колонки, що мають відповідні назви (А, Б, в), і для кожного рядка в датасеті це будуть нулі і одиниця в тій колонці, до якої вона належить.	Кількість текстових значень не більше певного числа N_0

Більшість систем IoT мають типові або незмінні шаблони даних. Для підвищення загального часу виконання попередньої обробки, пропонується формувати метадані вхідного датасету на етапі аналізу вхідного потоку та зберігати на сервері. Після формування алгоритму попередньої обробки на кроці «Визначення правил обробки», правила у декларативному поданні додаються до раніше сформованих метаданих та запис на сервері оновлюється.

При наступному запиті до серверу, метадані нового потоку повинні бути порівняні із вже збереженими метаданими. При знайденні співпадань, блок «Визначення правил обробки» пропускається, і очищення відбувається за вже сформованими правилами. Таким чином, при зберіганні порівняно невеликого обсягу даних, даний підхід дає значний вииграш у часі обробки через підвищення рівня автоматизації.

Переваги:

1. Підвищення достовірності кінцевого результату роботи мережі IoT.
2. Підвищення якості вхідних даних за рахунок виправлення втрат та видалення хибних записів.
3. Зменшення часу на попередню обробку даних за рахунок використання шаблонів обробки.

Недоліки:

1. Використання додаткових ресурсів для проведення попередньої обробки даних.
2. Застосування додаткової пам'яті сервера для зберігання шаблонів обробки.

Висновки. В даній роботі проаналізовано існуючі способи попередньої обробки вхідних датасетів та запропоновано зміни для підвищення ефективності та більш вигідного використання програмних та часових ресурсів. Сформовано критерії підбору алгоритмів очищення даних від випадково виникаючих помилок у заданому кроці процесу попередньої обробки даних. Рекомендовано використання шаблонів обробки на основі сформованих метаданих вхідного потоку для використання вже розрахованих алгоритмів очищення. У подальшій роботі буде розглянуто більш ефективне формування метаданих, їх формат та зберігання.

Література

1. Buhaienko Y., Globa L.S., Liashenko A., Grebinichenko M. "Analysis of clustering algorithms for use in the universal data processing system", OSTIS 2020.
2. R. Deepa. Methods and techniques to evaluate the performance of Data Cleansing Algorithms for very Large Database Systems / R. Deepa, Dr. R Manicka Chezian. // IJARCET. – 2016.
3. A Domain-Independent Data Cleaning Algorithm for Detecting Similar-Duplicates / Kazi Shah Nawaz Ripon Ashiqur Rahman and G.M. Atiqur Rahaman. // JOURNAL OF COMPUTERS. – 2010.
4. A Data Cleaning Method Based on Association Rules [Електронний ресурс] / W.Weijie, Z. Mingwei, Z. Bin, T. Xiaochun – Режим доступу до ресурсу: www.atlantis-press.com.

ВИКОРИСТАННЯ ОБЧИСЛЮВАЛЬНИХ ПОТУЖНОСТЕЙ МОБІЛЬНИХ ПРИСТРОЇВ ТА ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ У КОРПОРАТИВНІЙ МЕРЕЖІ

Смаглюк В.О., Алексєєв М.О.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: amxleclerk@gmail.com, alexeyev@its.kpi.ua

USAGE OF COMPUTING POWER OF MOBILE AND INTERNET OF THINGS DEVICES IN THE CORPORATE NETWORK

The using of free resources of computing devices in a heterogeneous network for the organization of distributed computing is an important approach, because due to advances in hardware development, the computing power of devices connected to the network increases, and delays because of their network interaction cease to have a critical negative impact. The proposed approach is based on the creation of a distributed cluster computing system such as volunteer computing or grid systems of personal computers. However, existing methods and software solutions have a number of disadvantages related to the mobility, cost or confidentiality of information. The advantage of the proposed approach is the using of unoccupied resources of Internet of Things devices, mobile and stationary devices in combination with software containerization technologies. The paper considers an experimental environment for studying the effectiveness of the approach.

Переважну частину часу електронні пристрої не використовуються на повну потужність своїх обчислювальних ресурсів або можливостей зі зберігання інформації. Перш за все це характерно для універсальних пристроїв на зразок персональних комп'ютерів та офісного обладнання, яке експлуатується з певною періодичністю. Для того, щоб задіяти ці ресурси існує декілька підходів. Насамперед, це обчислювальні кластери, ґрід-системи персональних комп'ютерів (ІСПК) та програмні рішення для волонтерських обчислень [1]. Стаціонарні кластери характеризуються високою ефективністю обчислювальних потужностей, однорідністю середовища та високою безпекою даних. Однак, мають високу сукупну вартість володіння (ТСО), особливо, якщо потреба в них виникає зрідка; ІСПК корпоративного рівня притаманні захист цілісності обчислень, висока мобільність, гетерогенність системи, стійкість до збоїв. Проте, налаштування системи вимагає специфічних навичок, відсутня структурована історія версій управляючого програмного продукту, що призводить до складності у технічній підтримці; системам для волонтерських обчислень на зразок BOINC характерні проблеми з цілісністю даних, оскільки обчислення поширюються за периметр організації, де їх важко відслідковувати.

Отже, щоб на основі незайнятих ресурсів пристроїв, підключених до корпоративної мережі, можна було реалізувати і ефективно використовувати обчислювальну систему, необхідно, щоб вона відповідала наступним вимогам: мала невисоку ТСО, водночас дозволяла використовувати ресурси досить різні за походженням і характеристиками (апаратне і системне

програмне забезпечення), враховувала часову та просторову мобільність пристроїв, що підключаються, мала високий рівень інформаційної безпеки обчислень та нескладне налаштування і підтримку системи.

Для того, щоб задовольнити ці вимоги було прийняте рішення про використання підходу для використання прикладних програмних компонентів у вигляді контейнерів. Контейнеризацію було обрано як основну технологію через ряд її переваг: ізолюваність та уніфікація компонентів, висока швидкість розгортання, менші вимоги до ресурсів, динамічний розподіл ресурсів, перевикористання та модифікація контейнерів, великий набір програмних компонентів, готових до використання.

З-поміж ряду доступних програмних продуктів націлених на створення необхідної обчислювальної системи було обрано Kubernetes. Перевагою цього продукту над іншими є комплексний набір інструментів для управління кластером, що дозволяє контролювати кожен аспект системи, а також повністю автоматичні процеси оркестрації та управління життєвим циклом елементів системи. Kubernetes використаний для управління робочими навантаженнями та послугами в контейнерах, що полегшує як декларативне налаштування, так і автоматизацію [2]. Kubernetes кластер оперує цими контейнеризованими застосунками, розподіляє навантаження між обчислювальними одиницями, слідкує за життєвим циклом кожної скомпільованої збірки за деякими параметрами: кількість одночасно розгорнутих сервісів, фактичне число доступних ресурсів до використання та ін. Головними компонентами Kubernetes кластеру є головний вузол (master node), який керує та управляє набором робочих вузлів та власне робочі вузли (worker nodes), що відповідають за запуск та контроль усіх подів (pods) та контейнерів кластеру.

Однак, для використання Kubernetes необхідно, щоб робочі вузли, об'єднані у групи, мали приблизно однакові апаратні та програмні характеристики і відключення робочого вузла сприймається системою як виключна ситуація, що відрізняється від вимог поставлених у роботі. Тому було прийнято рішення експериментально дослідити можливості системи в умовах, що відрізняються від тих, для яких вона була створена.

Експериментальний макет (див. рис. 1) містить один головний вузол, два робочі вузли та додатковий сервер керування (control server) з встановленим програмним забезпеченням Ansible, що допомагає поширювати команди на елементи кластеру централізовано [3].

Робочими вузлами представлено два пристрої. Цієї кількості достатньо для початкового налаштування та моделювання розподіленої системи. Кількість робочих пристроїв не обмежена. Робочі вузли мають різні цільові операційні системи (Ubuntu Desktop 20.04 на віртуальній машині, Raspberry Pi OS на мікрокомп'ютері Raspberry Pi 4 model B). Такий підхід симулює гетерогенну систему. Попередньо планувалася система із задіянням Android-смартфонів. Але, як з'ясувалося, на даний момент це завдання не можна виконати через відсутність у цій операційній системі підтримки критичних функцій необхідних для контейнеризації (cgroups, containerd) та управління

кластеру (kubelet). Часткові успіхи у цьому питанні є досить специфічними [6], але недостатніми для розвитку цієї ідеї як базової.

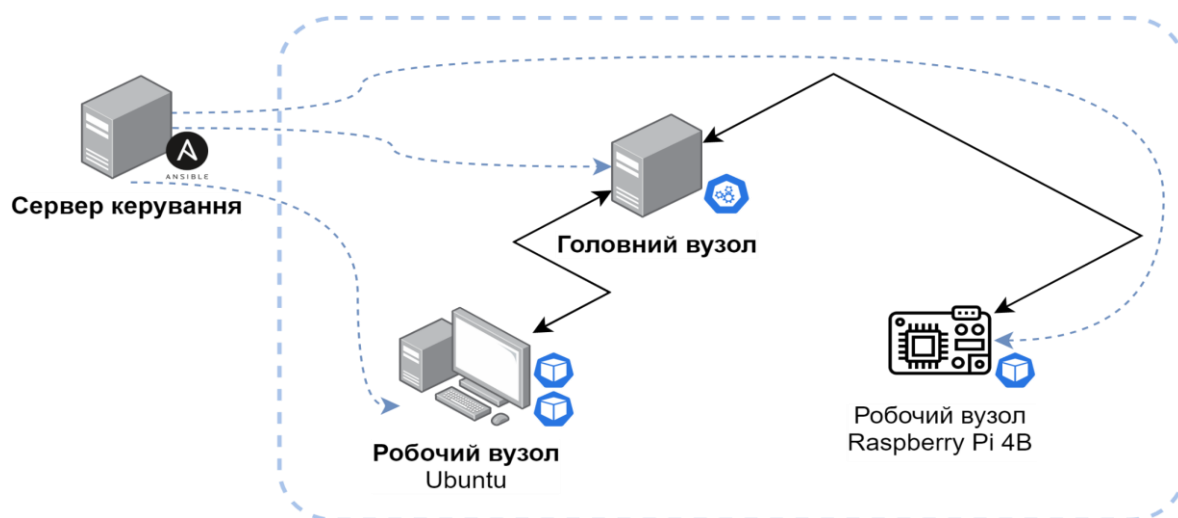


Рис. 1. Схема експериментального макету.

У даний момент за допомогою моніторингових інструментів (htop, Prometheus) відбувається збір даних від Kubernetes кластеру для того, щоб більш точно оцінити перспективність даної моделі обробки даних, виявити та проаналізувати проблемні аспекти та знайти варіанти їх вирішення. Головним параметром для дослідження є динаміка використання ресурсів робочих нод та рівень автоматизації системи.

Висновки. Проведене у роботі дослідження існуючих технологій на предмет можливості використання для створення обчислювальної системи з використанням незадіяних ресурсів пристроїв, підключених до корпоративної мережі, показало, що вибір програмного рішення Kubernetes є доцільним, оскільки технологія дозволяє використовувати апаратні і програмні обчислювальні ресурси різні за походженням і характеристиками, дозволяє їх підключати і від'єднувати у процесі експлуатації. Ефективність такого підходу та рівень інформаційної безпеки обчислень є напрямком для подальшого вивчення та аналізу.

Література

1. Mykola Alieksieiev, Vladyslav Shkola. Android-based Grid Computing Implementation.// Proceedings of the XII International Conference Dedicated to the 170th anniversary of Lviv Polytechnic National University, TCSET' 2014, Lviv-Slavske, Ukraine, February 25- March 01, 2014. p. 689-691.
2. Gaurav Gupta. Components of Kubernetes Architecture [Електронний ресурс] 2019 - <https://medium.com/@kumargaurav1247/components-of-kubernetes-architecture-6fee4d5c712>.
3. Ansible Documentation, Basic Concepts [Електронний ресурс] 2021 - https://docs.ansible.com/ansible/latest/network/getting_started/basic_concepts.html
4. StackOverFlow, Is it possible to run containers on android devices? [Електронний ресурс] 2019 - <https://stackoverflow.com/questions/53527277/is-it-possible-to-run-containers-on-android-devices>.

МОДИФІКОВАНИЙ АЛГОРИТМ ПОПЕРЕДНЬОЇ ОБРОБКИ НЕЧІТКИХ ЛОГІЧНИХ ПРАВИЛ

Бугаєнко Ю.М., Врачинська А.О.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

Email: yura.buhaenko@gmail.com; ars.vrachynska@gmail.com

THE MODIFIED ALGORITHM PRETREATMENT FUZZY LOGIC RULES

This report describes the problem of big data in information and telecommunication networks and the way to solve it using a decision-making system based on fuzzy logic. A modified algorithm for preprocessing fuzzy logical rules used in building a base of fuzzy logical rules is described.

В даній доповіді описана проблема великих даних в інформаційно-телекомунікаційних мережах та шлях її вирішення за допомогою застосування системи прийняття рішень на основі нечіткої логіки. Описано модифікований алгоритм попередньої обробки нечітких логічних правил що застосовується при побудові бази нечітких логічних правил.

Завдяки стрімкому розвитку можливостей обчислювальної техніки, об'єм даних не може являтися певним критерієм того, чи являються вони великими. Сьогодні великі дані вимірюються у терабайтах, а завтра – в петабайтах. Тому основною характеристикою Big Data є ступінь їх структурованості та варіантів представлення. Для обробки великих даних використовується багато сучасних інтелектуальних систем, але загальна складність та обробка даних в режимі реального часу продовжує залишатися одним із важливих недоліків для багатьох технічних галузей. Таким чином, телекомунікаційна галузь стикається з необхідністю обробляти, аналізувати та прогнозувати значні обсяги інформації, що характеризується значним неструктурованим, не одночасним прийомом даних з різних джерел. Теорія нечіткої логіки дає можливість описати набір правил, які нескладно використовувати для реальної системи. Використання нечіткої бази знань під час обробки потоку великих даних допомагає зменшити час обробки даних для систем прийняття рішень у реальних технічних галузях.

При роботі над системою прийняття рішень на основі бази нечітких знань, виникає проблема, коли після кластеризації даних ми отримуємо набори правил які містять в собі дублюючі та конфліктуючі елементи. Для побудови бази нечітких знань необхідно усунути ці неточності в правилах, для чого було вирішено використати алгоритми виявлення дублікатів та конфліктуючих правил.

Алгоритм побудови нечітких логічних правил складається з двох етапів: очищення дублюючих та конфліктуючих правил. Перший етап складається з формування правил, які можна зручно відобразити у вигляді таблиці з набором логічних правил, представлених у форматі Якщо ... Та ... То. Система не може містити правил, які містять однакові набори умов, тому

що вони будуть або дублювати одне одного, або перетинатися. Для реалізації використовуються кластери лінгвістичної змінної, яким належить певне числове значення. При такому підході можливе виникнення аномалій у вигляді суперечливих або надлишкових правил. Щоб вирішити цю проблему потрібно виключити надлишкове правило або замінити співпадаючі правила одним правилом. Для додаткового аналізу використовується підхід очищення правил.

Щоб сформувати унікальний масив правил бази нечітких знань потрібно об'єднати дублюючі правила. При роботі циклу, який проходить через весь масив правил, кожне правило додається у проміжну вибірку із початковою вагою 1. Кожне дублююче правило, яке зустрічається у вибірці, збільшує вагу дубліката, і не вноситься у результуючий масив. Конфліктуюче правило в даному наборі вводиться в проміжну вибірку як самостійне правило і обробляється аналогічно.

Робота даного алгоритму зображена на блок схемі (рис 1.), в результаті чого буде отриманий масив, який містить в собі унікальні правила із зазначенням їхнього впливу на роботу системи. Також, в отриманому проміжному наборі правил будуть знаходитися конфліктуючі правила, які будуть усунені на другому етапі алгоритму.

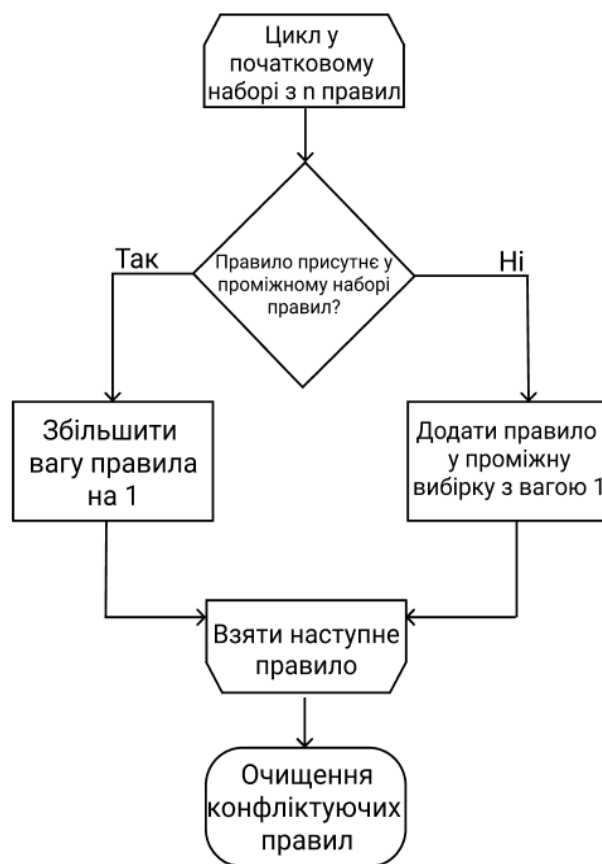


Рис.1. Блок-схема алгоритму очищення дублюючих правил.

На другому етапі для вирішення питання конфліктуючих правил було запропоновано алгоритм, в якому з набору суперечливих правил вибирається правило з найбільшою вагою. Правило залишається в наборі результатів, але його вага дорівнює середньому арифметичному всіх ваг суперечливих правил. Щоб швидко та зручно обчислити правило та усунути вплив початкової ініціалізації ваги правил та коефіцієнт росту ваги можна провести нормалізацію ваг правил в межах від 0 до 1. Блок схема роботи даного алгоритму зображена на рисунку 2.

На виході роботи алгоритму обробки правил було отримано новий набір, який не містить в собі суперечливих правил та дублікатів.

До переваг такого механізму можна віднести вирішення проблеми формування аномалій - очищення від надмірної ваги та надлишковості, тобто правила видаляються із врахуванням ваги кожного.

Недоліком такої системи є зменшення обчислювальної складності. Тобто при збільшенні кількості правил, зменшується точність у системі підтримки прийняття рішення. Також до недоліків можна віднести повільність використаного методу побудови нечітких логічних правил.

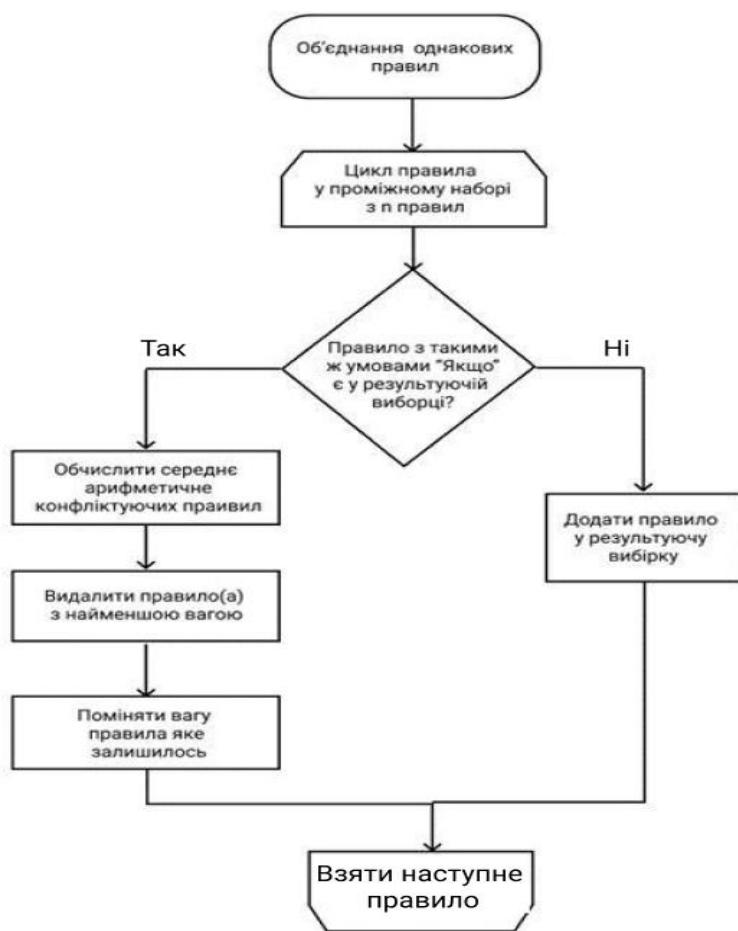


Рис.2. Блок-схема алгоритму очищення конфліктуючих правил.

Висновки. В даній статті було описано алгоритм побудови нечітких логічних правил на основі таблиці з набором логічних правил, представлених у форматі Якщо ... Та ... То, в ході чого був зроблений аналіз запропонованих методів очищення дублюючих та конфліктуючих правил. Також були виявлені певні переваги та недоліки такої системи. У подальшій роботі необхідно провести більш детальний аналіз алгоритму та запропонувати ефективне вирішення питання методу побудови нечітких логічних правил.

Література

1. Техническая коллекция Schneider Electric [Електронний ресурс]: – Режим доступу: <http://www.netkom.by/docs/N31-Nechetskaya-logika.pdf>
2. Савчук З.Р. «Засоби візуалізації складних логічних структур», Збірник матеріалів Міжнародної науково-технічної конференції «Перспективи телекомунікацій», Київ 2019.
3. Нечеткое моделирование и управление. А. Пегат с. [506-520].
4. Алтунин А.Е., Семухин М.В. Модели и алгоритмы принятия решений в нечетких условиях: Тюмень: Издательство Тюменского государственного университета, 2000, ст. 4-11.

МЕТОД ОБРОБКИ ІНФОРМАЦІЇ НА ОСНОВІ НЕЙРОМЕРЕЖ ДЛЯ МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ

Ушаков С.М., Курдеча В.В.

Інститут телекомунікаційних систем КПП ім. Ігоря Сікорського, Україна

E-mail: ushakovsergey21@gmail.com

A NEURAL NETWORK BASED INFORMATION PROCESSING METHOD FOR THE IOT NETWORK

IoT systems generate large volumes of diverse data that need to be processed and edited in a short time. One of the main challenges is the high traffic consumption due to the transfer of data to the cloud. Edge computing allows workloads to be redistributed from the cloud to a location near the data sources that need to be processed, saving time, increasing privacy, and reducing network traffic. This publication examines a method for compressing data in an IoT network through the use of a neural network.

Системи IoT генерують великі обсяги різноманітних даних, які необхідно обробити і відредагувати за короткий час. Однією з основних проблем є високе споживання трафіку в зв'язку з передачею даних в хмару. Обчислення на границі дозволяють перерозподіляти навантаження з хмари в розташування поблизу джерел даних, які необхідно обробляти, економлячи час, підвищуючи конфіденційність і скорочуючи мережевий трафік. У даній публікації розглядається метод стиснення даних в мережі IoT за допомогою нейронної мережі.

Хмарні обчислення, централізовано розгорнуті в глобальному масштабі, стали невід'ємною частиною обробки даних IoT. Однак Інтернет речей з хмарної підтримкою стикається з низкою труднощів, таких як затримки передачі, обмеження пропускної здатності і високе енергоспоживання. Наприклад, відправка одного біта даних у стільниковій мережі споживає занадто багато ресурсів, що скорочує термін служби системи IoT. З іншого боку, граничні обчислення стали перспективною парадигмою, яка штовхає хмарні служби на границю мережі. Її можна розглядати як децентралізоване хмарне середовище, що наближає обчислювальну потужність до джерела даних і дозволяє приймати локальні рішення.

Обчислення на границях в перспективі є кращим рішенням, ніж хмарні, в численних додатках IoT [1]. Наприклад, програми, що вимагають реакції в режимі, близькому до реального часу, такі як автономне водіння автомобілів і електронна охорона здоров'я, не можуть коректно працювати з хмарою через високу затримку і неефективну пропускну здатність, викликаними великою кількістю датчиків, підключених до мережі. Бездротові сенсорні мережі, бездротові тілесні сенсорні мережі і носимі пристрої становлять основні блоки архітектур IoT. Багато з цих "розумних" об'єктів, які відповідають за збір, обробку та передачу даних, все ще працюють від батарей і обмежені в ресурсах. Трьома основними складовими "розумних" об'єктів, є мікроконтролер, приймач і датчики. З усіх завдань добре відомо,

що передача даних є найбільш трафікоємною в IoT-вузлах [2,3]. Важливим кроком на шляху до зменшення надлишкового трафіку в додатках IoT є передача обчислювальних задач з хмари до границі, що оптимізує продуктивність мережі і підвищує приватність користувачів. Машина і глибоке навчання (deep learn) в області граничних обчислень можуть привнести численні поліпшення в традиційні підходи, засновані на хмарних обчисленнях:

- Обробка даних із використанням традиційних методів машинного навчання та передача результатів або необхідних функцій, отриманих із вихідних даних датчика.
- Розгортання частини слоїв мереж глибокого навчання на границі та передача вилучених функцій, розмір яких менший, ніж розмір вхідних даних.
- Розгортання нейронних мереж на границі з мінімальним розміром, зберігаючи точність.
- Навчання мереж у хмарі та доставка навчених моделей до границі.

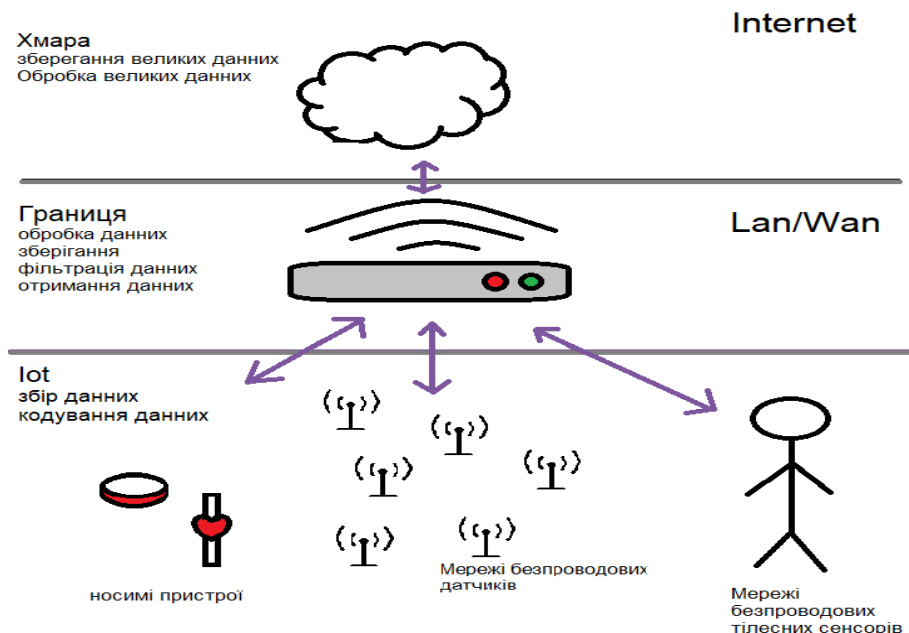


Рис. 1. Архітектура мережі IoT.

Основною задачею при обміні даними в мережах IoT залишається їх передача до хмарного середовища, що працює на базі систем зв'язку ближньої дії - персональних мереж. До них можуть відноситись як бездротові так і дротові мережі. До перших відносяться протоколи Bluetooth, NFC, RFID, Wi-Fi, Zigbee, Z-Wave, дротові ж мережі мають набагато ширший перелік технологій та назв так як сюди входять усі можливі промислові мережі та протоколи. На цьому етапі і виникає основна складність, що полягає у відносній повільності передачі даних до хмари та їх подальшій обробці у ній. Саме тому у даній роботі нас цікавлять архітектури мережі IoT, схожі до рис. 1, де дані збираються з інтелектуальних об'єктів, таких як носії і сенсорні пристрої, і періодично відправляються на прикордонний вузол по протоколам зв'язку короткого радіусу дії (наприклад, WiFi, Bluetooth).

Основним недоліком існуючих рішень, є те, що вони дають низький коефіцієнт стиснення даних із великою кількістю сенсорів. На даний час необхідна розробка методики стиснення даних для IoT-додатків і пристроїв з обмеженими ресурсами, ефективно працююча на багатовимірних часових рядах і реалізована на реальному носії.

Як варіант вирішення цих недоліків перш за все, треба застосовувати швидкий враховуючий помилки та втрати даних, компресор на зібраних даних перед передавачами, який розглядається як найбільший споживач трафіку в пристрої IoT (Рис.2.). На другому етапі потрібно відновлювати передані дані на крайовому вузлу і обробляти їх, використовуючи контрольовані методи машинного навчання.

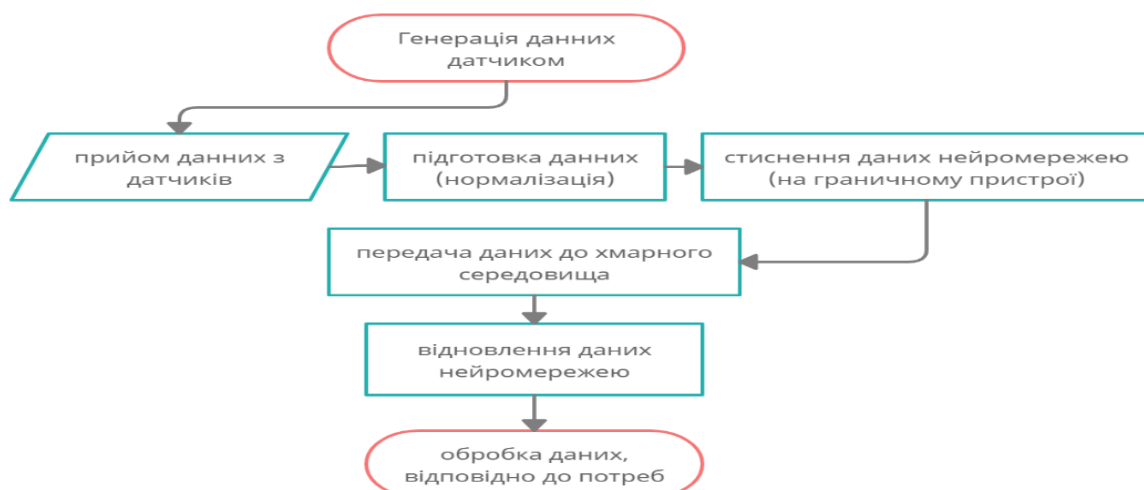


Рис. 2. Метод граничної обробки інформації на основі нейромереж для IoT.

Більшість пристроїв IoT в даний час оснащені кількома датчиками і здатні збирати різні типи даних. Таким чином, методи стиснення повинні працювати з даними з великою кількістю сенсорів на одному пристрої. Крім того, в разі додатків, що працюють в режимі реального або близького до реального часу, час відновлення (декомпресії) алгоритму має бути невеликим, щоб передати дані в модель машинного навчання і повернути результати прогнозування класифікації користувачеві в найкоротші терміни. Методи стиснення, засновані на перетворенні, змінюють необроблені дані на набір коефіцієнтів. Алгоритм стиснення повинен адаптуватися і добре працювати в різних додатках, суб'єктах і видах діяльності. Це приводить нас до висновку -кожна з представлених змінних, що міститься в даних, повинна відповідати умовам, необхідним для бездоганної роботи нейромережі, що не завжди є так.

Література

1. W. Shi, J. Cao, Q. Zhang, Y. Li, L. Xu, Edge computing: Vision and challenges, IEEE Internet Things J. 3 (5) (2016) 637–646, <http://dx.doi.org/10.1109/JIOT.2016.2579198>.
2. G. Anastasi, M. Conti, M.D. Francesco, A. Passarella, Energy conservation in wireless sensor networks: A survey, Ad Hoc Netw. 7 (2009) 537–568. ([http://refhub.elsevier.com/S0167-739X\(18\)33171-6/sb2](http://refhub.elsevier.com/S0167-739X(18)33171-6/sb2)).
3. M.A. Razzaque, C. Bleakley, S. Dobson, Compression in wireless sensor networks: A survey and comparative evaluation, ACM Trans. Sen. Netw. 10 (1) (2013) 5:1–5:44, <http://dx.doi.org/10.1145/2528948>, URL <http://doi.acm.org/10.1145/2528948>.

МЕТОД ВИЯВЛЕННЯ ВТОРГНЕНЬ В МЕРЕЖІ ІОТ

Гіззатуллін Д.Д., Курдеча В.В.

Інститут телекомунікаційних систем КПП ім. Ігоря Сікорського, Україна

E-mail: deny.gizz@gmail.com

THE METHOD FOR DETECTING INTRUSIONS INTO AN IOT NETWORKS

Modern network intrusion detection methods are analyzed. Considered the advantages and disadvantages of using a neural network method of intrusion detection. Prospects for the use of neural network methods are considered. Proposed scheme of intrusion detection system based on a neural network.

Проаналізовано сучасні методи виявлення вторгнень у мережу. Розглянуто переваги та недоліки використання нейромережевого методу виявлення вторгнень. Розглянуто перспективи використання нейромережевих методів. Запропоновано метод виявлення вторгнень на основі нейронної мережі.

По даним експертів [1] та аналітиків [2] кількість атак на мережі ІоТ зростає. За першу половину 2019 року серверам-пасткам, які видають себе за ІоТ пристрої, вдалось зафіксувати 105 млн атак на пристрої ІоТ, що приблизно в 9 разів більше ніж за аналогічний період 2018 року, де було зафіксовано 12 млн атак. Розвиток ІоТ нерозривно пов'язаний з ростом потенційно вразливих пристроїв. Користуючись слабким захистом ІоТ-продуктів, кіберзлочинці прикладають все більше зусиль для створення і монетизації ІоТ-ботнетів.

Одним із кроків направлених на підвищення безпеки, являється використання систем виявлення вторгнень. Дані системи спрямовані виявлення аномалій в мережевому трафіку, що являють собою небажаний зловмисний трафік.

В наш час системи виявлення вторгнень базується переважно на поєднанні сигнатурних та статистичних методів.

Сигнатурні методи дозволяють описати атаку на мережу певним набором правил, або за допомогою формальної моделі, яка наприклад може представляти собою семантичний вираз на спеціальній мові.

Суть даного методу полягає у використанні спеціалізованої бази шаблонів (сигнатур) атак для пошуку дій, що підпадають під визначення

“атака”. Такий метод може захистити від атак, сигнатури яких уже присутні в базі даних системи виявлення вторгнень. У виявленні аномалій значну роль відіграє вибір оптимальної кількості врахованих параметрів оцінки, а також визначення загального показника стану аномальності в захищеній системі [3].

Основним недоліком сигнатурних методів являється здатність системи виявити атаки невідомих типів. БД експертної системи повинна містити сценарії більшості відомих на сьогоднішній день атак.

Для того щоб усунути недоліки таких систем доцільно застосовувати клас методів виявлення вторгнень, який повністю покладається на статистичний апарат.

Статистичні методи основані на припущенні, що для певної системи існує свій профіль нормального стану і будь-які значні відхилення від цього стану являється ймовірним кандидатом на можливу атаку. Для побудови базового нормального профілю системи використовується статистичний набір даних, вільному від аномалій.

На відміну від сигнатурних методів, статистичні можуть виявляти нові типи мережевих атак, для яких ще не існує певної сигнатури. Системи виявлення вторгнень основані на статистичних методах не потребують оновлення сигнатурних БД, що значно спрощує експлуатацію системи.

Серед недоліків таких систем виявлення вторгнень можна відмітити складність завдання порогових значень, що являє собою не тривіальну задачу, яка потребує глибоких знань про підконтрольну систему. Статистичні методи нечутливі до порядку слідування подій[3].

Одним із варіантів усунення недоліків попередніх систем, може бути використання нейромережевих методів виявлення вторгнень. Всі методи виявлення вторгнень базуються на визначенні певного набору параметрів співставлення яких з параметрами функціонування мережі в певний момент часу дає змогу судити про наявність втручання в роботу мережі. Беручи до уваги здатність нейромереж оптимізувати свої параметри в ході свого навчання, можна вважати дослідження нейромережевих методів вельми перспективними.

На відміну від сигнатурних методів, нейромережі можуть самі визначати важливість певних параметрів, значення яких впливають на рішення про вторгнення в мережу, так як нейромережа, в ході свого навчання, встановлює

закономірності в атаках[3]. В той самий час мережа сама признає нормального функціонування мережі, і визначає порогові значення, відхилення від яких є небажаними в мережі.

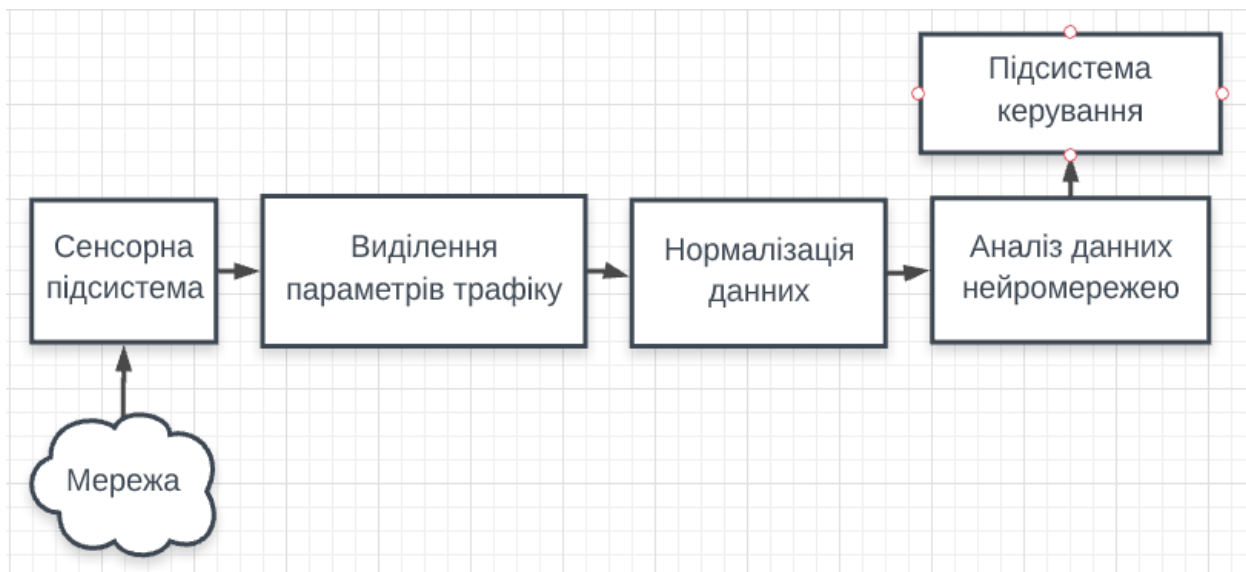


Рис. 1. Приклад схеми архітектури нейромережевої системи виявлення вторгнень.

На рис.1 запропоновано схему системи виявлення вторгнень на базі нейромережі.

Головною перевагою нейромережевих методів є можливість навчання з ціллю створення гнучких адаптивних систем. Також перевагою є можливість використання уже навчених ядер нейромереж, з наступним перенавчанням під власні цілі. Також на відміну від статистичних методів, деякі архітектури нейромереж здатні аналізувати часові послідовності.

Література

1. SECURELIST [Електронний ресурс] / Ден Деметр, Марко Пройсс, Ярослав Шмелев. Отчёт безопасности устройств за 2019 год — Режим доступа: <https://securelist.ru/iot-a-malware-story/94900/> (дата публикации: 19.12.2019).
2. Posetive Technologies [Електронний ресурс] / Актуальные киберугрозы. II квартал 2018 года — Режим доступа: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018-q2/> (дата публикации: 13.09.2018).
3. Шелухин О.И. Обнаружение вторжений в компьютерные сети (сетевые аномалии): учебное пособие для вузов / О.И. Шелухин, Д.Ж. Сакалема, А.С. Филинова. — М.: Горячая линия-Телеком, 2013. — 220 с.
4. M. Roopak, G. Yun Tian and J. Chambers, "Deep learning models for cyber security in IoT networks", pp. 0452-0457, 01 2019.

АНАЛІЗ МЕТОДІВ ЗАХИСТУ ДАНИХ В МЕРЕЖІ INTERNET OF THINGS

Петров О.С., Курдеча В.В.

Інститут телекомунікаційних систем КІІ ім. Ігоря Сікорського, Україна

E-mail: kyiv12@bigmir.net

ANALYSIS OF DATA PROTECTION METHODS ON THE INTERNET OF THINGS

With the constant increase in the number of "smart" devices, the vulnerability of data also increases. There are a number of vulnerabilities between them on the Internet of Things that can be exploited by attackers. The paper considers various methods of solving these weaknesses. An effective IoT connection with Blockchain is presented. As a result, a complete or partial solution to the existing problems of the Internet of Things.

При постійному зрості кількості «смарт» приладів зростає і вразливість даних. В Інтернеті речей існує низка вразливих точок, якими можуть скористуватися зловмисники. В роботі розглядаються методи протидії атакам на мережу IoT та захисту інформації. Запропоновано метод захисту інформації, що базується на технології Blockchain.

Є низка критичних аспектів, які прямо або вторинно впливають на інформаційну безпеку в IoT. Найперше – це організаційні заходи, такі як: створення і впровадження єдиної політики інформаційної безпеки підприємства з урахуванням всіх додатків і систем, розробка правил безпечного використання IoT-приладів і мереж, вдосконалення законодавчого забезпечення недоторканності приватного життя та особистої, державної та інших таємниць, державна і приватна стандартизація і сертифікація пристроїв, каналів передачі, сховищ інформації та прикладного ПО з обробки та аналізу даних.

Технічні інструменти захисту даних від витоків, втрат і перехоплення, управління, використання також потребують переконфігурації, де це необхідно. Має бути реалізація шифрування та/або інших криптографічних методів, персоналізація IoT-пристроїв з використанням унікальних ідентифікаторів ID, MAC-адрес, ключів і сертифікатів, що забезпечують досить високий рівень кібербезпеки без додаткових витрат, гнучкі політики управління доступом з багатофакторною авторизацією, резервування, реплікація, організація захищеного периметра і інші засоби інформаційної безпеки [1].

Обладнання, яке використовується в IoT мережах не завжди відповідає необхідним критеріям. Виробник повинен нести відповідальність зі своєї сторони за продукцію та її ціленаправленість. Для повної відповідності вимогам мають використовуватись сучасні і надійні інструменти програмної розробки (API, бібліотеки, фреймворки, протоколи...) і апаратні рішення (плати, контролери та ін.). Бажано скоротити кількість компонентів, необхідних для роботи обладнання, оскільки кожен додатковий елемент є потенційним джерелом вразливостей і фізичних поломок. Девайси мають реалізувати безпечну аутентифікацію, узгодження зашифрованих сеансів і перевірку аутентичності користувачів. Для того, щоб як найдовше зберігати надійність і актуальність складових систем виробник повинен забезпечити регулярний випуск оновлень ПО для усунення

знайдених і потенційно можливих вразливостей.

Незважаючи на те, що дана область діяльності непідконтрольна окремому користувачеві IoT-системи, а регулюється галузевими гігантами або цілими державами, вона дуже важлива для кінцевого клієнта - підприємства або фізичної особи. Тому необхідно повноцінно ввести стандарт, адже він регулює довіреність інформаційної та фізичної компонентів IoT-систем: надійність, функціональну безпеку, інформаційну безпеку, безпеку персональних даних, стійке функціонування в умовах атаки.[2] Тому за останні роки державні і міжнародні організації провели низку заходів для стандартизації і регламентування. Однак, питання кібербезпеки інтернету речей хвилюють не тільки державних чиновників. Питаннями сертифікації IoT-систем займаються і приватні компанії, а також незалежні експертні співтовариства. На жаль, сьогодні сертифікація ще не діє повноцінно.

Для підтримки тенденції захищеності даних в мережі Інтернету речей, відносно нової технології, не достатньо розглянути її зі сторони самостійної концепції та методів її реалізації. Ефективним буде використання симбіозу недавно створених технологій та реалізація нових на основі існуючих.

Цікава зв'язка Інтернету речей з технологією блокчейну. Вони можуть забезпечити високий рівень перевірки довіри для даних, що передаються. Основна ідея полягає у наданні пристроям ідентичності, яка може бути перевірена під час першої ініціалізації та протягом всього життєвого циклу. Можливості технологій блокчейну, які покладаються на протоколи ідентифікації пристроїв та системи репутації, мають великий потенціал для систем IoT. За допомогою протоколу ідентифікації пристрою кожен з них може мати власний відкритий ключ блокчейну та надсилати зашифровані повідомлення про виклики та відповіді на інші, тим самим активний девайс залишається під контролем своєї ідентичності. Крім того, вузол з ідентифікацією може розвинути репутацію або історію, які відстежуються блокчейном.

На відміну від бази даних, яка має одного адміністратора, блокчейн дозволяє набору різноманітних адміністраторів "реферувати" дані, так що жоден адміністратор не може зловмисно або випадково змінити або видалити дані. І як тільки адміністратори досягнуть консенсусу, дані захищаються блоками, які «прикуті» один до одного криптографічно, формуючи книгу, стійку до фальсифікації [3].

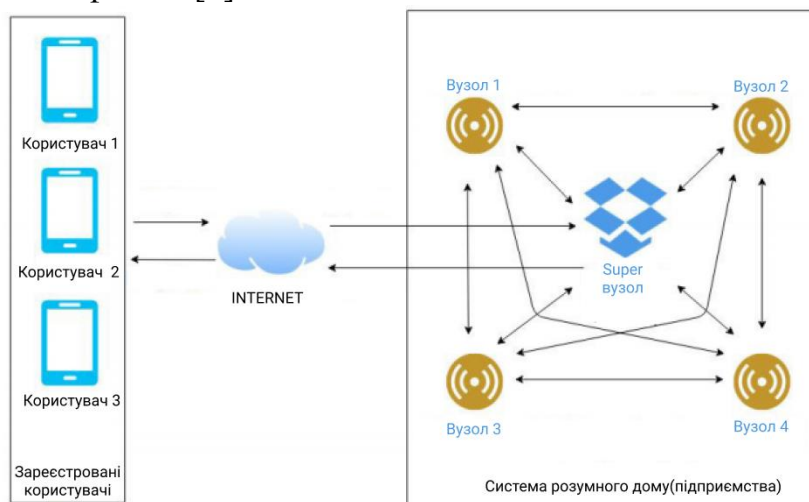


Рис 1. Архітектура розумного будинку з використанням IoT-Blockchain.

Пристрої IoT часто є легкою мішенню для розподілених атак DDoS. Під час DDoS-атак багато компрометованих комп'ютерних систем «бомбардують» ціль, таку як центральний сервер, величезним обсягом одночасних запитів, викликаючи цим відмову в обслуговуванні користувачів цільової системи.

Інша проблема сучасних мереж IoT - це масштабованість. Зі збільшенням кількості пристроїв, підключених через мережу IoT, сучасні централізовані системи для аутентифікації, авторизації та підключення різних вузлів у мережі перетворюються на вузьке місце. Це вимагає величезних інвестицій у сервери, які можуть обмінюватись великими обсягами інформації. Більше того, вся мережа може занепасти, якщо сервер стане недоступним.

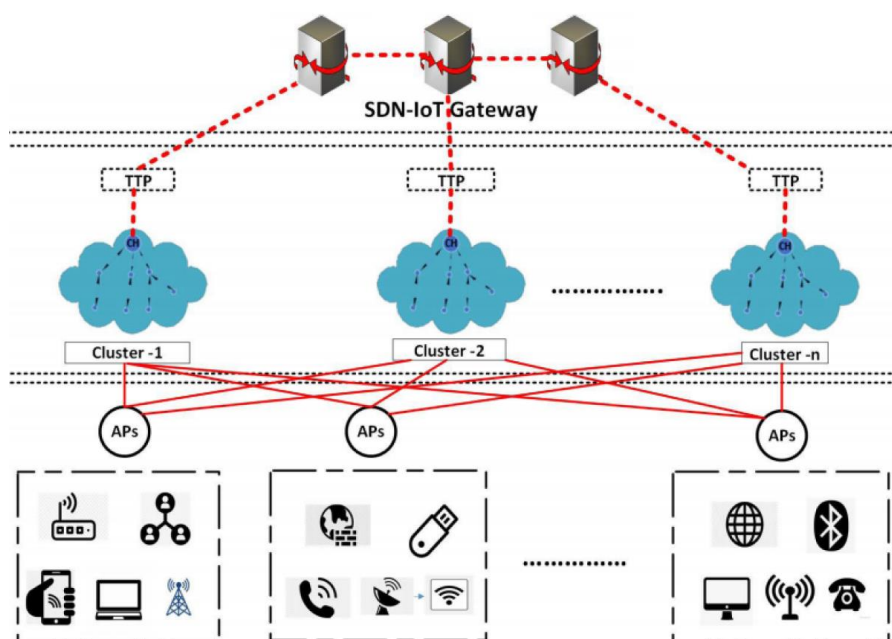


Рис. 2. Структура розподіленої системи Blockchain-IoT (рівень приладів, кластерний рівень, шлюзи хмарного рівня).

Таким чином, система складається з розподіленого цифрового реєстру, який ділиться між учасниками системи, який знаходиться в Інтернеті: транзакції або події перевіряються та реєструються в книзі, і їх не можна згодом змінити чи видалити. Це забезпечує спосіб запису інформації та спільного використання спільнотою користувачів. У межах цієї спільноти вибрані члени зберігають свою копію книги та повинні перевірити будь-які нові транзакції колективно через процес консенсусу, перш ніж їх прийматимуть до книги. Через розподіленість системи відпадають складнощі щодо масштабування та стійкості до DDoS-атак.

Література

1. Protecting Privacy and Data in the Internet of Things. Considerations and techniques for big data, machine learning and analytics / The Walbrook Building, London EC4N 8AF/ 2019 y.
2. Personal data protection for internet of things deployments: lessons learned from the European large-scale pilots of internet of things/ V.8.5, Create-IoT, Horizon 2020/ February 2020.
3. Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network/Saurabh Singh A., S. M. Sanwar Hosen , Byungun Yoon// presented at the IEEE January 14, 2021.

ПІДХІД ДО ОРКЕСТРУВАННЯ ВЕБ-СЕРВІСІВ У КЛАСТЕРІ, ЩО ВИКОРИСТОВУЄ РЕСУРСИ ПРИСТРОЇВ У КОРПОРАТИВНІЙ МЕРЕЖІ

Сегеда С.А., Алексєєв М.О.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: ti71segeda@gmail.com, alexeyev@its.kpi.ua

AN APPROACH TO WEB-SERVICES ORCHESTRATING IN A CLUSTER USING RESOURCES OF DEVICES CONNECTED TO CORPORATE NETWORK

The work is devoted to the topical problem of efficient execution of web services in a clustered environment. At the moment, there are solutions for orchestration of web services in a cluster, but they are intended primarily for clusters with a stationary architecture, while the use of resources of devices connected to the corporate network implies its frequent changes. The paper proposes an approach based on the use of the Nginx load balancer, which allows you to use the free resources of devices running various operating systems Windows, Linux, macOS connected to the network. The effectiveness of this solution was evaluated using the Artillery server throughput testing tools.

Робота присвячена актуальній проблемі ефективного виконання веб-сервісів у кластерному середовищі. На даний момент існують рішення з оркестрації веб-сервісів у кластері, але вони призначені насамперед для кластерів зі стаціонарною архітектурою, у той час як використання ресурсів пристроїв, що підключені до корпоративної мережі, передбачає її досить часті зміни. У роботі пропонується підхід на основі використання балансувальника навантаження Nginx, який дозволяє задіяти вільні ресурси пристроїв під керуванням різних операційних систем ОС Windows, Linux, macOS, що підключені до мережі. Ефективність такого рішення оцінена за допомогою засобів для тестування пропускної здатності сервера Artillery.

На сьогоднішній день, коли кількість сервісів в інтернеті зростає щосекунди, проблема продуктивності серверів, які їх обслуговують, стоїть дуже гостро. Проте, маючи певні ресурси, цю проблему досить просто вирішити на основі хмарних рішень, які дозволяють побудувати кластер майже будь якої потужності, який буде автоматично масштабуватись, виходячи з потреб. Але в умовах, коли необхідність у такому кластері епізодична, а у наявності є ресурси пристроїв, підключених до корпоративної мережі, більш вигідним може бути залучення простоюючих ресурсів пристроїв в мережі. Це не потребує вкладу грошей і в організаціях є в наявності багато не серверного обладнання - персональні комп'ютери, пристрої "розумного дому" та інтернету речей які не потребують автономності роботи та простоюють.

Отже, у роботі поставлена задача ефективного оркестрування веб-сервісів у кластері, побудованому на основі незадіяних ресурсів пристроїв, підключених до корпоративної мережі. Це гарантує найнижчу вартість

володіння такою системою, але передбачає можливість динамічно додавати або видаляти пристрої з конфігураційного файлу кластера чи балансувальника.

Аналіз існуючих рішень дозволив виділити наступні технології:

1. *Dynamic Configuration of Upstreams with the NGINX Plus API.*

Рішення для балансування навантаження між робочими нодами кластера с динамічною конфігурацією на основі програмного продукту Nginx plus. В цього сервісу є дуже широкий функціонал, що може задовольнити вимоги у динамічному конфігуруванні кластера [1], але це платний сервіс для великих компаній, ціна якого стартує від тисяч доларів на рік, що зводить нанівець його використання для вирішення поставленого завдання.

2. *Kubernetes.*

Засоби цієї системи для управління застосунками в контейнерах можна ефективно використовувати для оркестрації. Але Kubernetes зміни у конфігурації кластера сприймає перш за все як виключну ситуацію або це є наслідком автоматичного масштабування кластеру. І, що більш важливе, програмно-апаратні характеристики обчислювальних нод такого кластеру мають бути однаковими для групи нод, що є досить складним для предметної області даної задачі.

3. *Docker Swarm.*

Досить зручний інструмент для оркестровки, проте немає можливості динамічно змінювати конфігурацію кластера.

4. *Mesos.*

Працює за принципом Master - Slave, де є головний комп'ютер, який керує іншими. Проте також не можна динамічно додавати або видаляти slave з конфігурації.

5. *Nomad.*

Розроблений як альтернатива Kubernetes, проте технічно дане рішення відстає від Kubernetes.

6. *Flocker.*

Досить перспективний інструмент, проте розробка не продовжується починаючи з 2016 року.

7. *Helios.*

Підтримку завершено після виходу Kubernetes.

Результати аналізу існуючих рішень показують, що для вирішення поставленої задачі необхідно або адаптувати існуючі технології і найбільш релевантним у виборі виглядає Kubernetes, або ж спробувати створити власний оркестратор. У даній роботі розглянутий підхід на основі власної розробки.

Типовою архітектурою сучасного серверу може розглядатись наступна [2]: в нас існує кластер (сервер), у якому працює бізнес логіка, яка обслуговує застосунок. Для того, щоб запити могли потрапити всередину сервера необхідний балансувальник навантаження, наприклад Nginx або Apache HTTP Server [3]. Все, що робить балансувальник у більшості випадків, це перенаправляє запит у вказане місце, тобто в нашому випадку, на сервер з бізнес логікою. Проте, сервер може бути не один і балансувальник може розподілити запити між ними за заданим алгоритмом.

В даній роботі запропоновано використовувати алгоритм “Round Robin”. При цьому кожен сервер має свою “вагу” і запити розподіляються відповідно до неї [4].

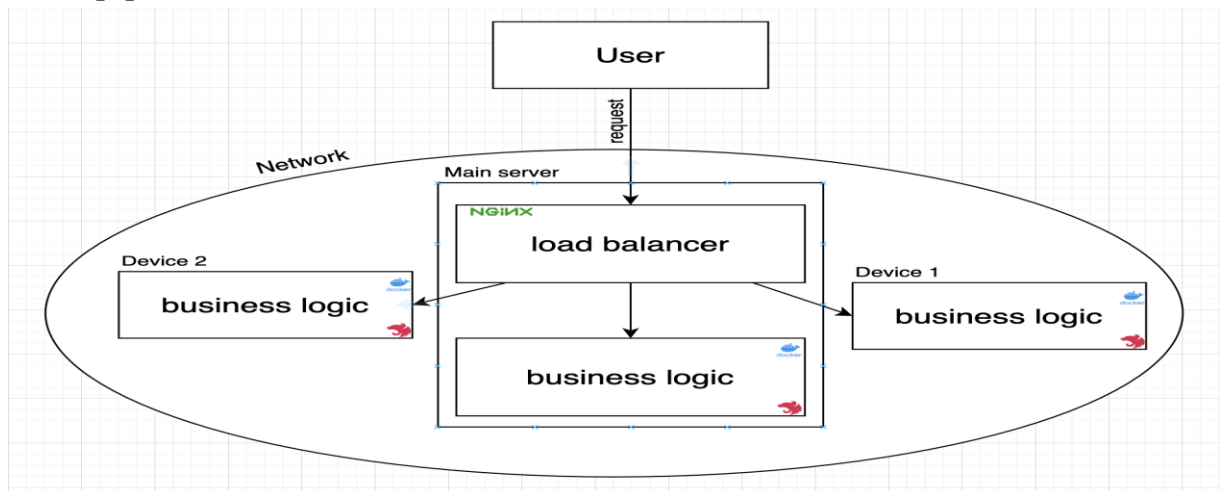


Рис.1. Структурна схема проекту.

Для вирішення поставленої задачі у роботі пропонується наступна архітектура. В нас є мережа, в якій знаходиться головний сервер, в якому в свою чергу знаходиться балансувальник та бізнес логіка упакована в Docker контейнер. Всі комп'ютери які ми хочемо застосувати також мають встановлений Docker і знаходяться в одній мережі з головним сервером, хоча останнє і не є обов'язковим. Docker зручно використовувати для контейнеризації застосунку, бо він дозволяє абстрагуватися від операційної системи, на якій буде запущено додаток, а також дозволяє запакувати все в образ, який потім може бути скачаний з репозиторія для їх зберігання, такого як Docker Hub або AWS ECR. При запуску головний сервер публікує посилання на певній адресі, перейшовши за яким починається завантаження скрипта, який після виконання скачує образ зі схожою бізнес логікою, встановить його та запустить. Бізнес логіка в свою чергу звертається в балансувальник з певним запитом. Для того щоб обробити цей запит використаємо CGI. CGI має певні переваги над іншими методами для зміни конфігурації під час роботи - це дуже легке рішення, яке не використовує

багато системних ресурсів, не потребує сторонніх технологій, функціоналу яких буде забагато для цих цілей, має багато варіантів реалізації на різних мовах програмування та не потребує багато зусиль в розробці [5]. Отримуючи запит, ми маємо ір адресу комп'ютера з якого цей запит було отримано і додаємо його до списку серверів, на які запити будуть транслюватися в подальшому.

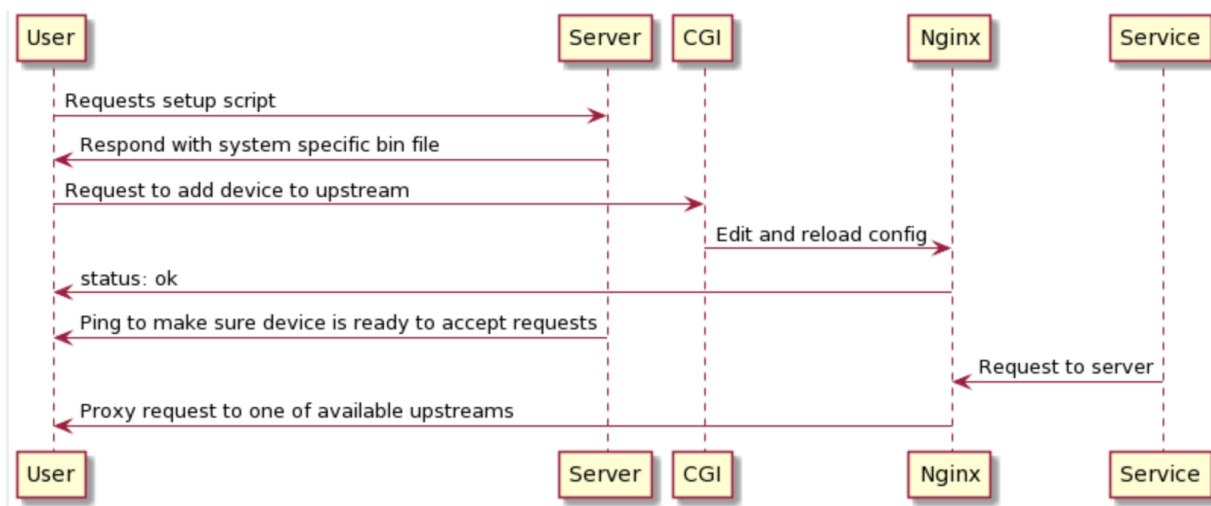


Рис.2. Діаграма станів проекту.

Після цього залишається лише перезавантажити конфігурацію і подальші запити будуть розподілятися між нашими серверами.

Висновки. Не дивлячись на наявність аналогів, запропоноване рішення має переваги над ними, а саме свою легкість у розробці, швидкодію, гнучкість і простоту та відчутно підвищити продуктивність сервера. Маючи не задіяні обчислювальні ресурси комп'ютерів підключених до мережі можна підключити їх до балансувальника навантаження та розподілити запити від користувачів між цими пристроями.

Література

1. Nginx documentation, "Dynamic Configuration of Upstreams with the NGINX Plus API", available at: [https://docs.nginx.com/nginx/admin-guide/load-balancer/dynamic-configuration-api/].
2. Chris Richardson, "Pattern: Microservice Architecture", 2020, available at: [https://microservices.io/patterns/microservices.html].
3. Nginx documentation, "What Is Load Balancing?", available at: [https://www.nginx.com/resources/glossary/load-balancing/#:~:text=A%20load%20balancer%20acts%20as,overworked%2C%20which%20could%20degrade%20performance].
4. Tony Mauro of F5, "Choosing an NGINX Plus Load-Balancing Technique", October 29, 2015, available at: [https://www.nginx.com/blog/choosing-nginx-plus-load-balancing-techniques/].
5. Nginx documentation, "FastCGI Example", available at: [https://www.nginx.com/resources/wiki/start/topics/examples/fastcgiexample/].

Секція 6. Сенсорні мережі та прикладні аспекти застосування
телекомунікаційних технологій

УДК 621.396.946

**УДОСКОНАЛЕННЯ МАТЕМАТИЧНОЇ МОДЕЛІ ОЦІНКИ
ЗВ'ЯЗНОСТІ ВУЗЛІВ МОБІЛЬНОЇ БЕЗПРОВОДОВОЇ СЕНСОРНОЇ
МЕРЕЖІ ІЗ ТЕЛЕКОМУНІКАЦІЙНИМИ АЕРОПЛАТФОРМАМИ**

Новіков В.І., Лисенко О.І., Алексєєва І.В.

Інститут телекомунікаційних систем КІП ім. Ігоря Сікорського, Україна

E-mail: novikov1967@ukr.net, lysenko.o.i.1952@gmail.com

**IMPROVEMENT OF THE MATHEMATICAL MODEL OF ASSESSMENT OF
CONNECTION OF MOBILE WIRELESS SENSORY NETWORK NODES WITH
TELECOMMUNICATION AIRPLANES**

The essence of improving the model, which determines its novelty, is that the proposed methods of joint use of a set of analytical models for assessing the reliability of data transmission in radio channels with a set of analytical models for predicting the movement of mobile sensor nodes. This allowed not only to assess the presence of connectivity of a given reliability, but also to predict its duration in a rapid and unpredictable change in the position of mobile sensor nodes.

Актуальним питанням на сьогодні є необхідність оперативної організації зв'язку в районах з відсутньою або зруйнованою мережною інфраструктурою в наслідок надзвичайних ситуацій природного чи техногенного характеру. Це можливо шляхом розгортання мобільних безпроводових сенсорних мереж (МБСМ) із використанням телекомунікаційних аероплатформ (ТАП). Особливо актуально застосування ТАП на основі мініатюрних безпілотних літальних апаратів (БПЛА), що є більш дешевими і оперативними на відміну від великих висотних аероплатформ [1].

Мобільні сенсорні вузли (МСВ) таких мереж можуть вільно переміщуватись в заданому районі та з'єднуватись між собою безпосередньо – у зоні радіо видимості, або із ретрансляцією пакетів через сусідні МСВ або ТАП, утворюючи таким чином багатоланкові мережі довільної структури [2]. Однак швидке та непередбачуване переміщення МСВ в таких мережах призводить до втрати зв'язності між ними, а отже до труднощів при побудові маршруту та передачі даних між ними. Для того, щоб визначити кожне наступне положення ТАП у просторі необхідно оперативно оцінити

наявність та час існування зв'язності кожної пари МА, що потребує удосконалення математичної моделі оцінки зв'язності вузлів МБСМ із ТАП.

Для удосконалення моделі оцінки зв'язності вузлів МБСМ із ТАП запропоновано поєднати аналітичні моделі для оцінки достовірності передачі повідомлень в радіоканалах з аналітичними моделями переміщення МСВ [3].

Показано, що максимальна дальність безпосереднього радіозв'язку між парою вузлів мережі обмежується, по-перше, енергетикою радіолінії, при якій відношення сигнал-шум в точці прийому не менше заданої величини для забезпечення заданої ймовірності пакетної помилки (PER) при заданому виді сигнально-кодової конструкції (СКК).

По-друге, максимальна дальність безпосереднього радіозв'язку між парою вузлів мережі визначається ефективністю методу множинного доступу (МД) до загального каналного ресурсу. Якщо протяжність радіолінії збільшується, то кількість колізій при організації МД зростає, а отже зростає затримка передачі та зменшується пропускна здатність. Тому максимальну дальність радіозв'язку можна визначити граничним значенням пропускної здатності каналу s^0 при заданих розмірі пакету даних L , інтенсивності трафіку G та швидкості передачі V . На довжину радіолінії ТАП-ТАП обмежень не має (окрім енергетики), оскільки метод МД, що використовується на ній, не залежить від нормованого часу поширення пакету.

Таким чином, для забезпечення заданих вимог до характеристик методів МД, потужність передавача слід обирати так, щоб забезпечити необхідний рівень PER на відстані, що визначається максимальним часом поширення пакету в стільниках МБСМ із ТАП.

Знаючи максимальну похилу дальність радіолінії МСВ-ТАП та допустимий кут місця для точці розміщення МСВ, можна визначити максимальний радіус стільника, створюваного ТАП. Так при куті місця 60^0 - 90^0 та при висоті ТАП $2600 \leq h < 3000$ м в щільно забудованому місті він становить $R \leq 1500$ м. Але враховуючи маневрування ТАП по колу з мінімальним радіусом та неточність його виводу, максимальний радіус зони стабільного покриття становитиме $R \leq 1450$ м.

Через свою мобільність МСВ не можуть постійно знаходитись в зоні радіо видимості інших МСВ і в зоні покриття ТАП, отже виникає практичний інтерес розрахунку тривалості зв'язності між МСВ, протягом якого вони можуть здійснювати інформаційний обмін. Для дослідження тривалості зв'язності між МСВ запропоновано декілька математичних моделей

переміщення МСВ в умовах прямої радіо видимості та з урахуванням ретрансляції. Визначимо *тривалість зв'язності* $T_{зв\ ij}$ пари вузлів (МСВ-МСВ або МСВ-ТАП) як час досягнення одним МСВ границі зони прямої радіо видимості з іншим МСВ (наприклад, час досягнення МСВ із точки B границі кола з центром в точці A та радіусом R , як показано на рис. 1). За допомогою математичного апарату тригонометрії матимемо наступне значення $T_{зв}$:

$$T_{зв} = \frac{AB \cos \varphi + \sqrt{R^2 - AB^2 \sin^2 \varphi}}{v},$$

де v – швидкість переміщення МСВ B , м/с; φ – кут напрямку переміщення МСВ B .

Таким чином тривалість зв'язності прямо пропорційна радіусу зони покриття та обернено пропорційна швидкості переміщення МСВ. На величину тривалості зв'язності також впливає характер мобільності МСВ. Було виконано моделювання переміщення МСВ за 4-ма сценаріями, що, описують, наприклад, рух пошукової бригади під час рятувальної операції (рис. 3):

- 1) «марш» ($\varphi = const$, $v = const$);
- 2) «випадкові напрямки» ($\varphi = const$, $v = const$);
- 3) «випадкове блукання в полі» ($\varphi = random$, $v = const$, $l = const$);
- 4) «випадкове блукання в місті» ($l = const$, $v = const$, $\varphi = random \{0^0, 90^0, 180^0, 270^0\}$).

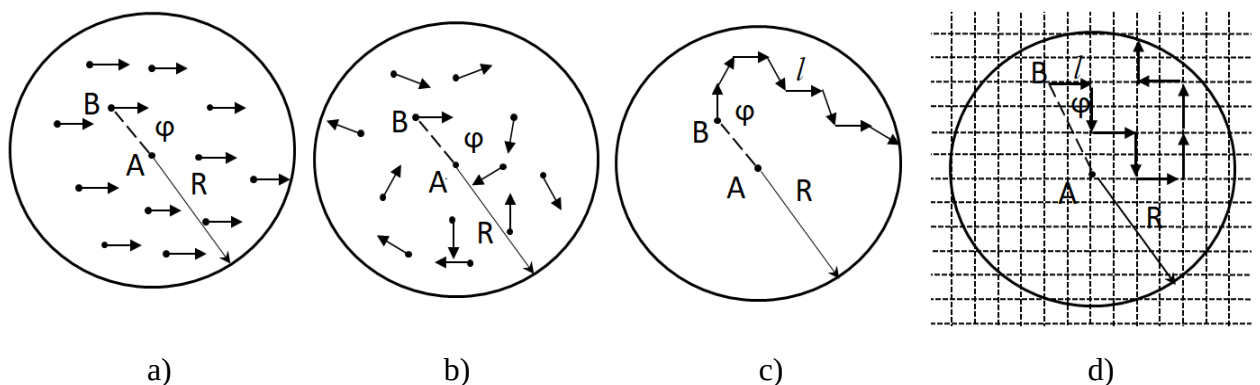
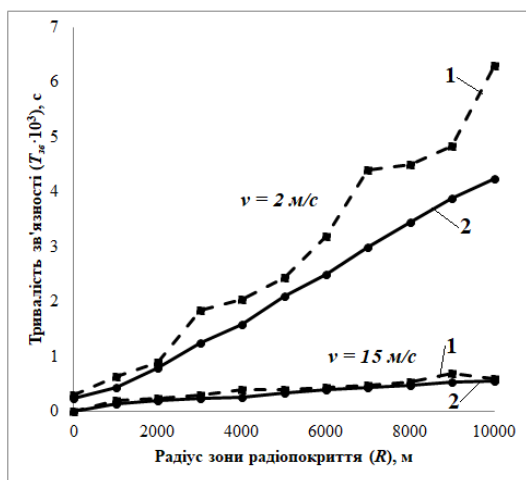
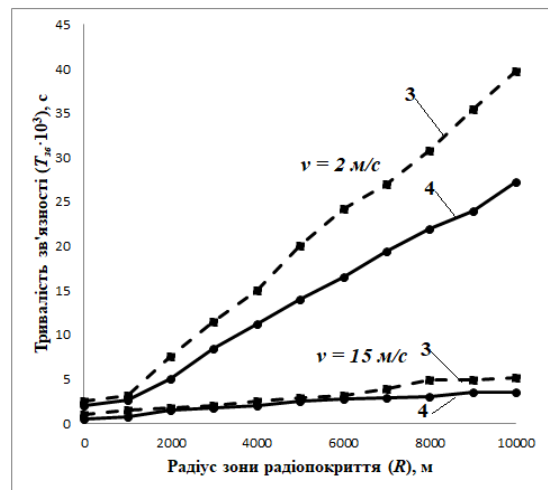


Рис. 1. Траскторії руху вузлів МБСМ із ТАП в залежності від сценарію мобільності:
1 – «марш» (а), 2 – «випадкові напрямки» (б),
3 – «випадкове блукання в полі» (с), 4 - «випадкове блукання в місті» (д).

Результати моделювання приведені на рис. 2.



а)



б)

Рис. 2. Залежність середнього часу досягнення МСВ границі зони покриття від радіусу зони при різних швидкостях і сценаріях переміщення: 1 – «марш» (а), 2 – «випадкові напрямки» (а), 3 – «випадкове блукання в полі» (б), 4 – «випадкове блукання в місті» (б).

Результати моделювання показують, що найбільші значення тривалості зв'язності відповідають сценарію «випадкове блукання в полі», а найменші – «випадкові напрямки» (при фіксованій швидкості переміщення вузлів v та радіусі зони покриття R). Так тривалість зв'язності з'єднання «ТАП-пішохід» на випадок «випадкових напрямків» становитиме в середньому 36 хв, а з'єднання «ТАП-транспортний засіб» - в середньому 5 хв.

Таким чином, удосконалена модель оцінки зв'язності вузлів МБСМ із ТАП дозволяє оцінювати наявність зв'язності між МСВ відповідно до заданої достовірності та прогнозувати її тривалість в умовах швидкого і непередбачуваного руху МСВ.

Література

1. Ильченко М. Е., Кравчук С. А. Телекоммуникационные системы на основе высотных аэроплатформ. – К.: Наук. думка, 2008. – 580 с.
2. Бунин С.Г., Войтер А.П., Ильченко М.Е., Романюк В.А. Самоорганизующиеся радиосети со сверхширокополосными сигналами. – К.: НПП «Издательство «Наукова думка» НАН Украины». – 2012. – 444 с.
3. Новіков В. І. Математичні моделі, методи і алгоритми оптимізації показників функціонування безпроводових сенсорних мереж із мобільними сенсорами та телекомунікаційними аероплатформами [Текст] / В.І. Новіков, О.І. Лисенко, С.В. Валуйський, О.Г. Гуйда // Вчені записки Таврійського національного університету імені В.І. Вернадського. – 2020. Том 31 (70) № 3 2020 Частина 1. – С. 54 – 64.

МЕТОД РЕАЛІЗАЦІЇ КОНЦЕПЦІЇ «CLEAR SPACE»

Явіся В.С., Лисенко О.І.

Інститут телекомунікаційних систем КІП ім. Ігоря Сікорського, Україна

E-mail: yavisya@bigmir.net

METHOD OF IMPLEMENTATION OF THE «CLEAR SPACE» CONCEPT

The creation of satellite systems for various purposes faces the problem of space debris, which is becoming more relevant every year. The development of ways to combat space debris is constrained by the need for significant investment in their implementation, as well as the lack of legal framework in this area at the international level. The use of low-orbit spacecraft in the form of a distributed satellite consisting of nanosatellites is proposed.

За допомогою супутникових систем можна здійснювати дослідження земної поверхні та верхніх шарів атмосфери, прогноз землетрусів, екологічний моніторинг, а також будувати системи супутникового зв'язку та навігації (ССЗН). Однак створення супутникових систем різного призначення стикається з проблемою космічного сміття, яка з кожним роком стає все більш актуальною.

На навколоземній орбіті за інформацією від різних джерел знаходяться понад 750 тисяч об'єктів, які являють собою не що інше як космічне сміття. У переважній більшості це різні гайки, болти і частки фюзеляжу, які рухаються зі швидкістю понад 28 тисяч км/годину. Серед них є і величезні старі супутники з ядерними елементами та розгінні блоки, які, як правило, відправляють на спеціальну орбіту поховання.

Існує кілька офіційних орбіт поховання. «Класична» розташовується на 200 км вище геостаціонарної орбіти, де знаходяться тисячі навколоземних супутників. На цю орбіту відправляються відпрацьовані орбітальні апарати для зменшення ймовірності їх зіткнення з робочими об'єктами.

Ще одна найбільша сміттєва орбіта для великих супутників знаходиться на висоті від 600 до 1 000 км. На цю орбіту відправляються військові розвідувальні супутники з ядерною енергетичною установкою. Вважається, що частини супутників зможуть перебувати на низькій сміттєвій орбіті понад дві тисячі років, після чого гравітація Землі поступово притягне активні реактори. Однак знаходження навіть на цій орбіті вимагає періодичної корекції траєкторії супутників, без якої їх перебування там може становити серйозну небезпеку і труднощі в подальшому дослідженні космосу.

Зараз тільки 10% всіх об'єктів космічного сміття фіксуються наземними станціями, а траєкторія їх руху відома. На навколоземних орбітах постійно відбувається так званий ефект Кесслера, коли одні шматочки сміття постійно стикаються з іншими, що призводить до абсолютно неконтрольованого поділу цих об'єктів. Згідно з математичними розрахунками, зіткнення двох космічних частин сміття призводить в середньому до появи ще шести-семи

невеликих об'єктів. Вчені вважають, що в майбутньому, якщо людство продовжить з такою швидкістю виводити об'єкти в космос, в тому числі на геостаціонарну орбіту, рано чи пізно станеться каскадний ефект: один космічний об'єкт зіткнеться з іншим, після чого він досить сильно змінює орбіту і стикається з іншими штучними об'єктами, які знаходяться на своїх орбітах. Гіпотетично це може буквально за кілька днів знищити або вивести з ладу всі супутники, створені людьми [1].

Крім того, деякі великі космічні об'єкти, у яких повністю закінчується термін експлуатації, навмисно підривають для того, щоб в подальшому їх невеликі уламки притягувалися Землею і згорали в атмосфері. Однак існують десятки прикладів, коли шматки сміття залишалися на орбітах, як в разі зіткнення двох штучних супутників «Космос-2251» та Iridium 339 в лютому 2009 року або тестування Індією своїх протисупутникових гармат в березні 2019 року.

На сьогоднішній день поки не існує дієвих технологій для боротьби з космічним сміттям, крім відправки супутників на орбіти поховань.

Безліч вчених працюють над створенням систем для утилізації космічного сміття. В основному такі проекти пропонують два рішення проблеми. Перше дозволяє збільшити термін керованого перебування супутників або їх частин, які відпрацювали свій ресурс, на сміттевій орбіті, але очевидно, що цей термін колись закінчиться. Друге – передбачає створення роботів-збирачів сміття, які будуть його виводити з орбіти Землі. Розвиток таких способів боротьби з космічним сміттям стримується необхідністю значних інвестицій на їх реалізацію, а також відсутністю законодавчої бази в даній сфері на міжнародному рівні.

Питання про чистоту у власному будинку ми вирішуємо дуже просто: зібрали сміття і винесли на смітник. Однак є альтернативне рішення забезпечення чистоти, яке впливає з давно знайомого постулату: «Чисто не там, де прибирають, а там, де не сміять». Стосовно до космосу це означає, що всі об'єкти, виведені на навколоземну орбіту не будуть там кинуті, а після виконання своєї місії будуть утилізовані.

Для забезпечення ефективного використання штучних апаратів висока вартість їх створення і виведення в космос, як правило, компенсується досить тривалим періодом експлуатації. Крім технічних вимог до розташування супутників на певній висоті, це одна з причин використання середніх і високих орбіт – чим вище орбіта, тим довше на ній може знаходитися супутник. Низькі навколоземні орбіти не можуть забезпечити тривале перебування супутників в космосі без коригування траєкторії руху внаслідок їх досить швидкого зниження, яке викликане гальмуванням апаратів частинками атмосфери, які присутні на таких орбітах. Однак саме низька орбіта здатна забезпечити самоочищення космосу, коли супутники після виконання своєї місії будуть опускатися в атмосферу природним чином і згоряти в ній. Такий підхід вимагає перегляду самих принципів побудови космічних апаратів (КА), оскільки на сьогодні, в своїй переважній більшості, це великогабаритні об'єкти, які не зможуть повністю згоріти при вході в атмосферу.

В даному випадку для створення ССЗН актуальним стає використання КА у вигляді розподіленого супутника, який складається з угруповання над малих КА, відомих під назвою наносупутник (НС) [2].

Орієнтацію НС може забезпечувати система на двигунах-маховиках, а їх розвантаження буде виконуватись моментним магнітопривідом. Однак, лише компактні іонні прискорювачі дозволять НС змінювати орбітальну позицію або утримуватись на ній тривалий час.

Також двигуни малої тяги можуть використатися для керованого сходу з орбіти ушкоджених НС. Це змусить їх згоряти в атмосфері Землі й частково вирішить проблему космічного сміття.

Важливим етапом створення, підтримання та оновлення ССЗН є процес виведення супутників на орбіту, який, як правило, відбувається за допомогою ракет-носіїв, в тому числі багаторазового використання. Наприклад, останній запуск для поповнення угруповання системи *Iridium* відбувся 11.01.2019 року з космодрому База Ванденберг. За допомогою ракети-носія *Falcon 9* було виведено десять супутників *Iridium NEXT*, вагою 860 кг кожен. Всього протягом 2017-2019 років відбулось вісім запусків *Falcon 9*, що дозволило здійснити виведення 75 апаратів [3]. Зазначений спосіб виведення є досить вартісним, тому лише держави з потужною економікою мають власні ракети-носії.

Альтернативний спосіб виведення супутників на орбіту – повітряний старт, який передбачає запуск космічних апаратів з повітряних суден горизонтального зльоту. Таки переваги, як зменшення маси, сили протидії та вартості ракети-носія, дозволяють у кілька разів знизити витрати на запуск. На сьогодні саме українські літаки АН-124-100 «Руслан» та АН-225 «Мрія» можуть бути задіяні для виконання цієї місії. Зазначений спосіб є найбільш ефективним саме при виведенні на низьку орбіту [4].

Висновки. При використанні розподілених КА з'являється можливість поетапного оновлення космічного сегменту з меншими витратами. Використання НС вирішить проблему космічного сміття, оскільки НС будуть знаходитись на низькій орбіті та по закінченні своєї місії будуть повністю згорати в земній атмосфері.

Література

1. Святослав Иванов. Орбита захоронения: почему над Землей летают тысячи никому не нужных спутников. /Электронный ресурс/ <https://hightech.fm/2019/08/26/orbita-satellite>.
2. Olexandr Lysenko, Miroslov Sparavalo, Olena Tachinina, Valerii Yavisyia, Sergiy Ponomarenko. Feasibility Reasoning of Creating Ultra-Low Orbit Communication Systems Based on Small Satellites and Method of Their Orbits Designing // Information and Telecommunication Sciences, №1, 2020. – P. 59-70. DOI: <https://doi.org/10.20535/2411-2976.12020.59-70>
3. Все спутники связи. Каталог. /Электронный ресурс/ <http://ecoruspace.me>.
4. Lysenko, O.I., Tachinina, O.M., Yavisyia, V.S., Alekseeva, I.V. Concept of Construction of Satellite Communication and Navigation System clear Space. IEEE 6th International Conference, «Methods and Systems of Navigation and Motion Control», Kyiv, Ukraine, October, 22-24, 2020).– K.: NAU, 2020. – pp. 110–113.

СТРУКТУРА РОЗПОДІЛЕНОГО ТЕЛЕКОМУНІКАЦІЙНОГО СУПУТНИКА

Явіся В.С., Лисенко О.І.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: yavisya@bigmir.net

STRUCTURE OF DISTRIBUTED TELECOMMUNICATION SATELLITE

Large spacecraft will not be able to burn completely in the atmosphere. Therefore, it is proposed to build a spacecraft in the form of a distributed satellite, which consists of a group of nanosatellites. When using low orbits, the proposed solution generally increases the reliability of the entire system. It is also possible to gradually upgrade the space segment.

Для забезпечення самоочищення космосу та вирішення проблеми космічного сміття доцільно використовувати низькі орбіти. Однак при цьому космічні апарати (КА) великих розмірів не зможуть повністю згоріти в атмосфері. Тому для створення системи супутникового зв'язку (ССЗ) пропонується побудова КА у вигляді розподіленого супутника, який складається з угруповання наносупутників (НС).

Для визначення структури розподіленого супутника пропонується розглянути найбільш відому низькоорбітальну ССЗ *Iridium*. В ній функціонують понад 70 супутників, 66 з яких є активними. Вони розміщуються на 6-ти приполярних орбітах. Розроблений для цієї мережі механізм між супутникових зв'язків дозволяє передавати сигнал з одного супутника на інший без ретрансляції цього сигналу на Землю. У наземний сегмент входять дві центральні станції управління і контролю. Вони здійснюють управління орбітальним угрупованням КА, забезпечують синхронізацію ССЗ, організовують групові тракти передачі [1, 2].

Антенні системи КА *Iridium NEXT* формують 48 парціальних променів, які створюють загальну зону покриття діаметром понад 4000 км. Одна зона має діаметр близько 700 км.

Для виключення дублювання від сусідніх космічних апаратів частина променів виводиться з активного режиму роботи. В середньому кожен апарат створює близько 32 парціальних променів (сот) [3].

Середня пропускна здатність при використанні смуги частот 10,5 МГц для зв'язку між мобільним терміналом і супутником становить понад 110 каналів на одну соту поверхні Землі [3]. Для обслуговування абонентів можливості апарата дозволяють створити до 5700 телефонних каналів, але їх реальна кількість становить близько 3840. Враховуючи таке обмеження, в мережі на супутниках *Iridium NEXT* можливе одночасне обслуговування 253440 абонентів.

Пропонується створити НС угруповання, яке буде складатись з кластерів. Кожен кластер за об'ємом виконуваних функцій буде аналогічним супутнику системи *Iridium*. За таких умов, для створення глобальної системи

супутникового зв'язку необхідно буде розташувати на шести орбітах мінімум 66 кластерів НС (по 11 на кожній орбіті).

Склад кластеру із НС може бути не однорідним з погляду на функції, що виконуються окремими апаратами: основна частина НС може використовуватися для зв'язку із абонентськими терміналами, інші – для концентрації і комутації навантаження всередині кластеру, зв'язку із сусідніми кластерами НС, які розташовані на власній та суміжних орбітах, а також для зв'язку із наземними станціями. Оскільки відстань між НС кластеру складає лише кілька десятків метрів, взаємодія між ними може здійснюватися за допомогою *Wi-Fi* або оптичного сигналу [4]. Склад кластеру пояснює рис.1.

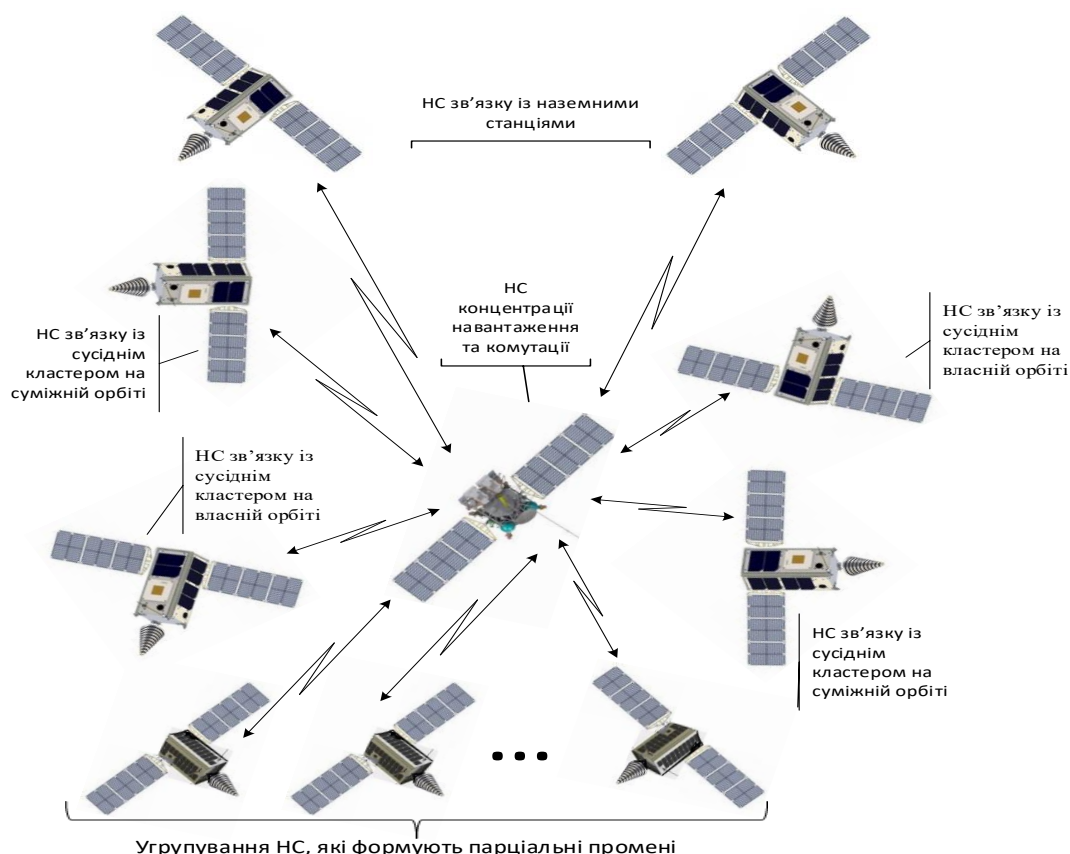


Рис.1. Склад кластеру із НС.

Мінімальна кількість НС у одному кластері визначиться наступним чином. Для зв'язку із абонентськими терміналами, за умови формування одним НС одного парціального променя, потрібно 32 апарати. Функцію концентрації і комутації навантаження всередині кластеру буде виконувати один НС (бажано із дублюванням). Для зв'язку із іншими кластерами на власній та суміжних орбітах – чотири НС, для зв'язку із наземними станціями – два НС. Таким чином, для виконання функцій аналогічних за обсягом тим, що виконує супутник *Iridium NEXT*, в кластері повинно бути не менше 40 НС.

При побудові ССЗ на базі кластерів НС, яка є схожою на систему *Iridium* та має лише шість орбіт, потрібно зазначити, що вони повинні

знаходитись на висоті близько 350 км. При менших висотах внаслідок кривизни Землі не можливо забезпечити покриття діаметром 4000 км, а тому необхідно збільшувати кількість орбіт, що приведе к збільшенню вартості системи та ускладненню управління нею.

Для формування діаграми спрямованості, яка забезпечить обслуговування території, що за площею співвідноситься із зоною обслуговування одного парціального променя супутника *Iridium NEXT*, можна використати фазіровану антенну решітку або параболічну антену. Але такий підхід виявляється неприйнятним у випадку застосування НС в наслідок значних ваго габаритних показників зазначених антен, тому пропонується використовувати спіральну конічну антену.

За умови знаходження НС на висоті 350 км для покриття зони діаметром 700 км, залежно від розташування такої зони відносно кластеру НС необхідна антена із шириною діаграми спрямованості θ від 30° до 60° . Для середньої частоти взаємодії НС і абонентського терміналу 1,6 ГГц та діаметрі спіралі $d=6$ см при $\theta=60^\circ$ довжина антени $l=13$ см, її підсилення становить $G=7-8$ дБ. У згорнутому стані така антена являє собою пружину, що займатиме об'єм близько $V=8$ см³, тобто 0,8 % від загального об'єму НС формату *CubeSat-1*.

Антени НС, що формують парціальні промені на межі зони обслуговування кластеру, повинні забезпечити ширину діаграми спрямованості до $\theta=30^\circ$, при цьому підсилення становить $G=13-15$ дБ, але довжина антени збільшиться до $l=56$ см при тому ж діаметрі. Тоді у складеному вигляді об'єм антени збільшиться майже у 4 рази [4].

Такий підхід дозволяє вирішити питання створення спрямованої діаграми для НС при мінімальних ваго габаритних показниках антенної системи.

Використання розподіленого супутника дозволяє підвищити надійність усієї системи, оскільки втрата або вихід з ладу окремих НС незначним чином вплине на характеристики угруповання, а у випадку часткового резервування НС в кластері такі події можуть бути повністю нівельовані. Немаловажним є і той факт, що з'являється можливість поетапного оновлення космічного сегменту.

Література

1. SatcomDV. Информация о системах спутниковой связи. /Електронний ресурс/ http://www.satcomdv.ru/informaciya_o_sistemah_sputnikovoj_sa.
2. Alexander Lysenko, Valerii Yavisiya, Andrii Tureichuk, Irina Alekseeva. Monitoring system and fixed communication on the basis of nanosatellites //2018 5th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T). October 10-13, 2018, Kyiv, Ukraine, pp. 495-498.
3. Satlink. Технические характеристики спутниковой системы связи Iridium /Электронный ресурс/ http://www.satlink.ru/Spytnikovaia_sviaz/Iridium/Tekhnicheskie_harakteristiki.html.
4. Lysenko, O.I., Tachinina, O.M., Yavisiya, V.S., Alekseeva, I.V. Concept of construction of satellite communication and navigation system clear space. IEEE 6th International Conference, «Methods and systems of navigation and motion control», Kyiv, Ukraine, October, 22-24, 2020).– K.: NAU, 2020. – pp. 110–113.

СИСТЕМИ ЖИТТЕЗАБЕЗПЕЧЕННЯ ТЕЛЕКОМУНІКАЦІЙНОГО НАНОСУПУТНИКА

Явіся В.С., Лисенко О.І.

Інститут телекомунікаційних систем

КІІІ ім. Ігоря Сікорського, Україна

E-mail: yavisya@bigmir.net

TELECOMMUNICATION NANOSATELLITE LIFE SUPPORT SYSTEMS

The creation of a satellite communication and navigation system based on distributed telecommunications satellites, which are a cluster of a certain number of nanosatellites, is possible only if the problem of ensuring their controlled position in orbit, as well as reliable energy supply. An approach to the construction of a stabilization and orientation system, as well as a power supply system is proposed

Створення системи супутникового зв'язку та навігації на базі розподілених телекомунікаційних супутників, які являють собою кластерне угруповання певної кількості наносупутників (НС), можливе тільки у випадку рішення завдання забезпечення керованого положення НС на орбіті, а також надійного енергозабезпечення [1].

Система орієнтації телекомунікаційного або навігаційного НС повинна будуватись виключно на активних методах, які реалізують за допомогою двигунів-маховиків, моментного магнітопривіду або реактивних двигунів (РД). Причому РД вимагають наявності на борту значних запасів палива, тому, останнім часом широко застосовують іонні двигуни (ІД), для роботи яких необхідна на порядок менша кількість палива, ніж для звичайних РД.

Для оцінки ефективності активних методів орієнтації зробимо ряд уточнень. НС стандарту CubeSat являє собою куб з ребром $R = 0,1$ м та масою близько $m_{нс} = 3$ кг. При використанні двигунів-маховиків на одній осі розташовується два маховики, які працюють синхронно. При реалізації моментного магнітопривіду для орієнтації по одній осі необхідне застосування двох котушок, розташованих під прямим кутом одна відносно іншої. ІД розташовуються на краю поверхні певних сторін CubeSat. Оскільки, для системи на двигунах-маховиках зміна швидкості обертання маховиків відбувається майже миттєво, при розрахунках цей час можна не враховувати. У свою чергу робота систем з моментним магнітопривідом та з ІД фактично відбувається в два однакові за тривалістю етапи – на першому відбувається розгін до певної кутової швидкості обертання, а на другому – гальмування [2].

Тоді, можна показати, що кут повороту НС навколо певної осі для різних систем орієнтації визначають наступні вирази:

- для системи на двигунах-маховиках:

$$\alpha_{nc}(t) = 3 \frac{m_m r^2}{m_{nc} R^2} \omega_m t \quad (1)$$

де m_m – маса маховика; r – радіус диска маховика; ω_m – швидкість обертання маховика;

- для системи з моментним магнітопривідом:

$$\alpha_{nc}(t) = \frac{3IpSB}{2m_{nc} R^2} t^2 \quad (2)$$

де I – струм котушки; p – число витків котушки; S – площа рамки котушки; B – індукція магнітного поля Землі;

- для системи з ІД:

$$\alpha_{nc}(t) = \frac{3F}{4m_{nc} R} t^2 \quad (3)$$

де F – сила, що розвивається ІД.

Зазначимо, що для системи на двигунах-маховиках кут обертання є лінійною функцією часу, а для систем з моментним магнітопривідом та з ІД – залежність квадратична. Для порівняння активних систем були обрані наступні значення параметрів, що входять до формул (1-3): $m_m = 0,02$ кг, $r = 0,03$ м, $\omega_m = 1,16$ рад/с (в середньому 4000 обертів за хвилину), $I = 0,43$ А, $p = 100$, $S = 0,005$ м², $B = 30$ мкТл, $F = 100$ мкН.

Часова залежність величини кута повороту для певної системи із урахуванням зазначених вище допущень представлена на рис. 1.

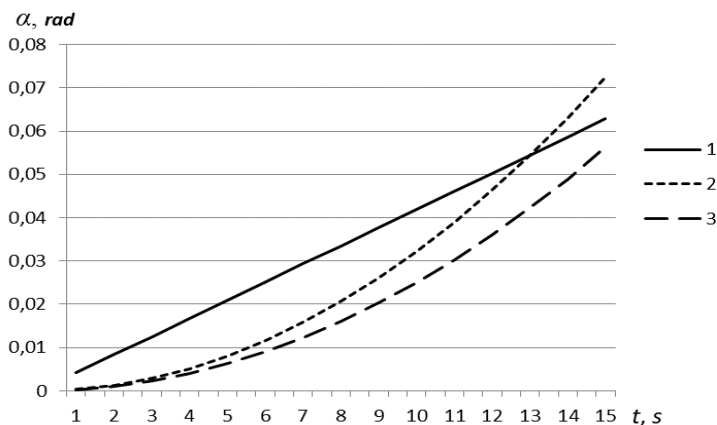


Рис. 2. Часова залежність величини кута повороту НС: 1 – для системи на двигунах-маховиках, 2 – для системи із моментним магнітопривідом, 3 – для системи з ІД.

Виходячи з характеристик, які наведені на рис. 1, можна заключити, що всі три системи володіють приблизно однаковими можливостями на інтервалі часу до 15 с, впродовж якого кутове положення НС змінюється майже на 0,7 рад або 4 градуси. Причому добір параметрів та аналіз проведений за умови, що системи мають близькі ваго-габаритні характеристики та показники енергоспоживання. Але кожна із систем має певні недоліки: системи на двигунах-маховиках потребують періодично здійснювати їх розвантаження; системи із моментним магнітопривідом не

забезпечують одночасну тривісну орієнтацію, що пов'язано із структурою магнітного поля Землі; системи з ІД мають ресурс роботи, який обмежений запасами палива.

З погляду на це обґрунтованим буде одночасне використання хоча б двох систем. Оскільки системи орієнтації на двигунах-маховиках та магнітних виконавчих органах не дозволяють здійснювати зміну орбіти НС, найбільш доцільним буде використання комбінованої системи, яка може бути реалізована в двох варіантах. В першому, вона складається з двигунів-маховиків та ІД, в другому – з магнітних котушок та ІД. Двигуни-маховики або магнітні котушки дозволяють вирішувати завдання стабілізації й орієнтації. ІД в першому варіанті реалізації будуть задіяні, в основному, для періодичного розвантаження двигунів-маховиків, в другому – для допомоги системі з моментним магнітопривідом виконувати одночасну тривісну орієнтацію. Але в обох варіантах ІД забезпечать можливість зміни орбіти НС, що в цілому дозволить значно збільшити їхній термін служби, а також здійснювати плановий відхід з орбіти по закінченні експлуатації [2].

Безперервне функціонування НС потребує певного енергозабезпечення. Зазвичай, основними споживачами є приймально-передаюче обладнання та система орієнтації НС.

Загасання для ідеальної ізотропної антени у вільному просторі визначається:

$$L = 32,4 + 20 \lg(f) + 20 \lg(d), \quad (4)$$

де f – частота в МГц, d – відстань в км.

Тому на межі зони обслуговування кластеру (відстань понад 1500 км) загасання становить $L = 160$ дБ.

Чутливість сучасних приймачів терміналів персонального супутникового зв'язку близько -118 дБ. Враховуючи підсилення спіральної антени до $G=15$ дБ, втрати, що пов'язані із формуванням спіральною антеною сигналу із круговою поляризацією – порядку 3 дБ, а також можливі втрати в атмосфері до 3 дБ, потужність випромінювання із «запасом» в 3 дБ повинна становити:

$$P = 160 - 118 - 15 + 3 + 3 + 3 = 36 \text{ дБ}, \quad (5)$$

тобто 4 Вт. Коефіцієнт корисної дії (ККД) передавача, як правило, не перевищує 30%, що відповідає потужності споживання 14 Вт. Додатково для роботи приймача потрібно 5 Вт.

Необхідне взаємне розташування променів НС в кластері можна забезпечити лише при керованому польоті НС. Гібридна система орієнтації та стабілізації споживає близько 4-8 Вт. При цьому необхідно врахувати той факт, що частина електричної потужності витрачається на підзарядку акумулятора, який забезпечує роботу НС під час знаходження його в тіні Землі. Виходячи з цього, сонячна батарея повинна забезпечити потужність живлення на рівні 45 Вт [1, 3].

Потужність потоку сонячного випромінювання на вході в атмосферу Землі, складає близько 1366 ват на квадратний метр [4]. На сьогодні

переважна більшість виробників сонячних батарей представляють продукцію з коефіцієнтом корисної дії (ККД), що не перевищує 20%, хоча є заяви про нові гелієві сонячні панелі, виготовлені із застосуванням нанотехнологій та нових напівпровідникових матеріалів з ККД до 35% [3, 5].

За умов розташування поверхні сонячної батареї НС перпендикулярно напрямку поширення сонячних променів (із допуском на незначне відхилення до 15 градусів), електрична потужність, яка виробляється, може бути знайдена:

$$P = 1366 \times \eta \times S, \quad (6)$$

де η – ККД сонячної батареї; S – площа поверхні сонячної батареї.

Для отримання необхідної потужності живлення площа поверхні сонячної батареї повинна бути не меншою, ніж:

$$S = \frac{P}{1366 \times \eta}, \quad (7)$$

тобто $S = 0,165 \text{ м}^2$. Стандартний розмір НС формату *CubeSat-1* – куб із стороною 10 см. За умови використання двох симетричних батарей, одна сторона якої дорівнює зазначеним 10 см, інша, за умови округлення розрахункового значення у більший бік, кратний 10 см – повинна мати довжину 90 см. Виходячи з цього та враховуючи необхідність наявності акумулятора у конструкції НС, його формат можна визначити як *CubeSat-2*, коли в одному кубі будуть розташовані елементи енергоукомплектування (сонячні батареї та акумулятор), а в іншому – обладнання відповідно до функціонального призначення.

Таким чином, особливості основних систем життєзабезпечення телекомунікаційного наносупутника наступні: кероване положення НС на орбіті може бути забезпечено шляхом використання комбінованої системи, яка може бути реалізована за допомогою двигунів-маховиків або магнітних котушок та ІД; для забезпечення питомого електроспоживання конструкція НС не може бути за форматом меншою ніж *CubeSat-2*.

Література

1. Lysenko, O.I., Tachinina, O.M., Yavisya, V.S., Alekseeva, I.V. Concept of construction of satellite communication and navigation system clear space. IEEE 6th International Conference, «Methods and Systems of Navigation and Motion Control», Kyiv, Ukraine, October, 22-24, 2020).– К.: NAU, 2020. – pp. 110–113.
2. V.S. Yavisya, N.M. Bendasiuk. Analysis of Methods for Orientation and Stabilization of Nano-Satellites // 4th International Conference methods and systems of navigation and motion control (MSNMC-2016), October 18-20, 2016, Kyiv, Ukraine, pp. 158-161. ISBN 978-1-5090-1052-3.
3. Alexander Lysenko, Valerii Yavisya, Andrii Tureichuk, Irina Alekseeva. Monitoring system and fixed communication on the basis of nanosatellites //2018 5th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T). October 10-13, 2018, Kyiv, Ukraine, pp. 495-498.
4. Энциклопедия по машиностроению XXL /Электронный ресурс/ <http://mash-xxl.info/info/495944>.
5. Солнечные батареи в космическом пространстве / Электронный ресурс/ <http://solarb.ru/solnechnye-batarei-v-kosmicheskom-prostranstve>.

АНАЛІЗ МЕТОДУ ВИЯВЛЕННЯ ТОЧКОВИХ ЦІЛЕЙ НА ОСНОВІ МОДЕЛІ ІНФРАЧЕРВОНОГО ПАТЧ-ЗОБРАЖЕННЯ

Неуймін О. С., Соколов К.А., Маленчик Т.В.

Радіотехнічний факультет КПІ ім. Ігоря Сікорського, Україна

E-mail: o.s.neuimin@gmail.com

ANALYSIS OF THE POINT TARGETS DETECTION METHOD ON THE BASIS OF THE INFRARED PATCH-IMAGE MODEL

The relevance of the detecting point targets problem on an image is presented. The infrared patch-image algorithm is briefly described. The results of point target detection modeling on the basis of the infrared patch-image model are presented.

Безпілотні літальні апарати (БПЛА) набувають швидкого розвитку, популярності та доступності. Відповідно, з'явилися нові потенційні небезпеки: використання БПЛА для введення незаконної відеозйомки, проникнення на заборонену територію, загроза для повітряного транспорту [1]. Отже виникає потреба у розробці сучасних систем, які були б здатні виконувати задачі виявлення цілі. Оптична система спостереження, що поєднує у собі функції цифрової обробки зображень та радіолокації, має здатність виявляти БПЛА та інші точкові об'єкти в умовах поганої видимості, на великих відстанях, в складних погодних умовах. Тому вона є корисна у військовій, екологічній, охоронній та інших сферах. Вище вказане представляє актуальність розробки відповідних методів виявлення для систем та комплексів відеоспостереження, які були б здатні зменшити ризики від діяльності БПЛА.

Усі відомі методи можна умовно поділити на два види - «супроводження до виявлення» та «виявлення до супроводження» [2]. Методи, які використовують принцип «виявлення до супроводження» не потребують процедури накопичення кадрів чи знання про швидкість, траєкторію чи форму цілі, а рішення про виявлення цілі приймається у кожному кадрі. При цьому, на основі моделі зображення, що складається з цілі f_T , фону f_B і шуму f_N (1) запропоновано чимало методів, таких як: методи виявлення по одному кадру, методи, що базуються на помітності цілі, методи виявлення цілі на основі рівня патч-зображення, методи засновані на вейвлет перетворенні, методи, що засновані на міжкадровій різниці [3].

$$f_0(x, y) = f_T(x, y) + f_B(x, y) + f_N(x, y), \quad (1)$$

де x та y координати пікселів. Серед цих методів найкращими показниками ефективності виявлення цілі володіє метод на основі моделі інфрачервоного патч-зображення (ІРІ) [4]. Метод дозволяє отримати менше залишкових шумів і завад для різноманітних фонів в порівнянні з класичними методами TopHat, MaxMean та MaxMedian, що дає змогу зменшити ймовірність хибної тривоги при заданій ймовірності виявлення цілі. Тому оцінка можливості його використання при виявленні точкових

цілей системою відеоспостереження представляє актуальність.

Метод ІРІ використовує модель зображення, яка відрізняється від традиційно прийнятої (1). В цій моделі, зображення перетворюється на патчі – частинки довільного розміру, на які поділене зображення. Нова модель зображення D описує ціль T , фон B та шум N , як патч-зображення. На основі формули (1) створюється нова модель зображення:

$$D = T + B + N. \quad (2)$$

При цьому T є розрідженою матрицею, а B - низькорангова матриця. Для правильного виявлення цілі необхідно отримати зображення самої цілі f_T . Це зображення отримується шляхом реконструкції патч-зображення цілі T шляхом вирішення задачі оптимізації (3) за допомогою методу прискореного проксимального градієнту (4) [4].

$$\min_{B, T} \|B\|_* + \lambda \|T\|_1 + \frac{1}{2\mu} \|D - T - B\|_F^2, \quad (3)$$

де $\|\cdot\|_*$ - ядерна норма матриці (сума сингулярних значень), $\|\cdot\|_1$ - l_1 -норма, $\|\cdot\|_F$ - норма Фробеніуса, λ – вагова константа, μ - ваговий параметр.

$$B_0 = B_{-1} = 0; T_0 = T_{-1} = 0; a_0 = a_{-1} = 0; \mu_0 > 0; \bar{\mu} > 0; \eta < 1.$$

$$Y_k^B = B_k + \frac{a_{k-1}-1}{a_k} (B_k - B_{k-1}); \quad Y_k^T = T_k + \frac{a_{k-1}-1}{a_k} (T_k - T_{k-1});$$

$$G_k^B = Y_k^B - \frac{1}{2} (Y_k^B - Y_k^T - D); \quad (U, S, V) = \text{svd}(G_k^B); \quad B_{k+1} = UJ_{\frac{\mu_k}{2}}[S]V^T;$$

$$G_k^T = Y_k^T - \frac{1}{2} (Y_k^B - Y_k^T - D); \quad T_{k+1} = J_{\frac{\mu_k}{2}}[G_k^T]; \quad (4)$$

$$a_{k+1} = \left(1 + \sqrt{4a_k^2 + 1}\right) / 2; \quad \mu_{k+1} = \max(\eta\mu_k, \bar{\mu});$$

$$\text{conv}_{k+1} = \|D - B_{k+1} - T_{k+1}\|_F / \|D\|_F; \quad B = B_k; \quad T = T_k.$$

Процес реконструкції патч-зображення цілі припиняється у випадку, коли модуль різниці між двома значеннями конвергенції не стане меншою деякого числа ε , $|\text{conv}_{k+1} - \text{conv}_k| < \varepsilon$.

Для аналізу алгоритму виявлення точкової цілі згенеровано зображення за моделлю (1), що складається з цілі, фону і шуму. Інтенсивність та розміри точкової цілі формуються на основі двовимірної гаусівської моделі

$$f_T(x, y) = I_{\max} \exp\left(-\frac{1}{2}\left[\frac{x^2}{\sigma_x^2} + \frac{y^2}{\sigma_y^2}\right]\right), \quad \text{де ціль представлена величиною пікової}$$

інтенсивності $I_{\max}$, а σ_x , σ_y - параметри горизонтальної та вертикальної протяжності. Шум генерується на основі розподілу Релея. Приклад зображення показано на рис. 1. Розмір зображення складав 480x640 пікселів. Відношення сигнал-шум становив 20 дБ, а $\sigma_x = \sigma_y = 0.8$.

Для оцінки ефективності роботи алгоритму визначалися швидкість виконання (кількість ітерацій алгоритму k та час виконання t), кількість хибних відміток N_f , наявність цілі (yes, no) в залежності від величини ε , від розміру патч-зображення p_s , та від кроку ковзного вікна w_s (табл.1).



Рис. 1. Приклад зображень до та після оброблення.

Таблиця 1. Результати моделювання.

При $ps = 25 \times 25$, $ws = 20 \times 20$					При $\varepsilon = 0.1$, $ws = 20 \times 20$					При $\varepsilon = 0.1$, $ps = 35 \times 35$				
ε	K	t ,мс	N_f	ціль	ps	K	t ,мс	N_f	ціль	ws	K	t ,мс	N_f	ціль
0.2	1	1250	9433	yes	20x20	4	1382	18	yes	10x10	4	7755	0	no
0.15	3	1528	1	yes	25x25	4	1600	0	yes	15x15	4	4419	0	no
0.1	4	1600	0	yes	35x35	4	2238	0	yes	20x20	4	3000	0	yes
0.01	6	1834	11	yes	55x55	4	4314	0	yes	25x25	4	1675	9	yes
0.001	7	2003	29	yes	75x75	4	7775	0	yes	30x30	4	1459	116	yes
0.0001	39	5478	146031	yes	95x95	4	14580	0	yes	35x35	4	1300	687	yes

З результатів моделювання (табл.1) видно, що значне зменшення величини ε приводить до зростання числа хибних відміток, та збільшення часу оброблення зображення. При $\varepsilon = 0.1$ відсутні хибні відмітки, а тривалість оброблення 1600 мс. Збільшення розмірів патч-зображення до $ps = 95 \times 95$ приводить до значного зростання тривалості оброблення зображення $t = 14580$ мс, а низькі значення до появи хибних відміток. При наближенні розмірів ковзного вікна до розмірів патч-зображення $ps = 35 \times 35$ з'являються хибні відмітки, однак зменшується тривалість оброблення, а при малих значеннях $ws = 10 \times 10$ алгоритм не виявляє точкову ціль. Таким чином, параметри алгоритму ІРІ необхідно підлаштовувати для заданих ситуацій та вимог виявлення точкової цілі.

Література

1. O. Neuimin, I. Tovkach and S. Zhuk, "Analysis of the Algorithm for Detecting a Point Object on a Sequence of Video Images Using Decisive Statistics of Marks," 2019 IEEE 39th International Conference on Electronics and Nanotechnology (ELNANO), Kyiv, Ukraine, 2019, pp. 690-693, doi: 10.1109/ELNANO.2019.8783530.
2. Yang, Huanhai. Detection and Tracking of Infrared Dim Small Image Sequence Moving Target. The Open Automation and Control Systems Journal 7, 2015, no. 1: 1698–1704.
3. Rawat, S. S., Verma, S. K., Kumar, Y. Review on recent development in infrared small target detection algorithms. Procedia Computer Science, 167, 2020, 2496–2505.
4. Gao, C., Meng, D., Yang, Y., Wang, Y., Zhou, X., Hauptmann, A. G. Infrared Patch-Image Model for Small Target Detection in a Single Image. IEEE Transactions on Image Processing, 22(12), 2013, 4996–5009.

АНАЛІЗ ЗАГРОЗ ТА МЕТОДІВ ЗАХИСТУ МЕРЕЖ ВІД XSS АТАК ТА SQL ІН'ЄКЦІЙ

Валуйський С.В., Собко Т.А.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: valuisnyi.stanislav@iit.kpi.ua

ANALYSIS OF THREATS AND METHODS OF PROTECTING NETWORKS FROM XSS ATTACKS AND SQL INJECTION

The article describes common threats that come from XSS attacks and SQL injection and possible damage they may cause. It also suggests effective methods of preventing these attacks and protection against them.

XSS-атаки та SQL-ін'єкції є одними із найпоширеніших видів атак на веб-додатки на веб-сайти. Вразливості до цих атак радикально знижують рівень захищеності інформації в системі (додатку). В даній статті проводиться огляд можливих загроз та наслідків цих атак, а також наводяться ефективні методи убезпечення від них.

Атаки типу XSS використовуються для наступних злочинних дій:

- крадіжка Cookies – дозволяє перехопити конфіденційні значення cookies користувача та індикатори сесії, які потім можуть бути використані для підробки сесії і несанкціонованого входу в систему;
- крадіжка даних з форм – перехоплення значень, які користувач вводить у поля форм на веб-сайті. Серед них може бути така критична інформація як логіни та паролі, дані кредитних карток, ідентифікаційні номери, інші дані які потім можуть бути використані у злочинних цілях;
- підробка контенту – внесення зловмисником змін у зовнішній вигляд та наповнення сторінок веб-сайту; може використовуватись як різновид фішингу, для реалізації попередньо описаної крадіжки даних (щоб спровокувати користувача ввести дані у підробне вікно), для несанкціонованого показу власної реклами на чужому веб-сайті та ін.

Також, з використанням XSS можуть реалізуватись інші види атак – DDoS-атака, підробка міжсайтових запитів (CSRF / XSRF)

XSS-атаки розділяють на два види – пасивні та активні.

Пасивні атаки відбуваються коли жертва переходить за спеціальним чином згенерованим посиланням, яке містить в собі зловмисний код (часто зашифрований). Для реалізації атак цього виду зазвичай використовується соціальна інженерія (наприклад, маскування повідомлення із посиланням під

важливий лист, розсилка в соцмережах, розміщення посилання на форумах).

Убезпечення від таких атак лежить у площині інформаційної грамотності кожного конкретного користувача. Це такі правила, як: не переходити за підозрілими посиланнями, не відкривати повідомлення із невідомих та підозрілих джерел, не натискати на кнопки і рекламні посилання на ненадійних веб-сайтах (наприклад, сайтах з піратським контентом).

Активні XSS-атаки є більш небезпечними, оскільки їх важко, або й неможливо, помітити. При такій атаці зловмисний код впроваджується в базу даних або який-небудь файл на сервері. Таким чином, всі відвідувачі сайту автоматично стають жертвами. Інтеграція може бути здійснена зокрема за допомогою SQL-ін'єкції (описано далі). Загалом, вразливість до атак цього виду присутня скрізь, де веб-програма використовує вхідні дані користувача для генерування вихідних даних, без достатнього рівня фільтрації, перевірки та кодування.

Захист від таких вразливостей має бути реалізований при розробці, з використанням наступних правил [1]:

- не дозволяти вставку ненадійних даних (даних користувача) ніде, окрім дозволених місць, та не приймати код JavaScript із ненадійних джерел;
- кодувати всі ненадійні дані перед вставкою їх до дозволених місць. До цього відноситься:
 - кодування HTML перед вставкою ненадійних даних у вміст HTML-елемента,
 - кодування атрибутів перед вставкою ненадійних даних у значення загальних атрибутів HTML,
 - кодування JavaScript перед вставкою ненадійних даних у значення даних JavaScript,
 - кодування значення JSON у контексті HTML та зчитування даних за допомогою JSON.parse,
 - кодування CSS перед вставкою ненадійних даних у значення властивостей стилю HTML,
 - кодування URL перед вставкою ненадійних даних у значення параметрів URL в HTML,
- якщо дані, які вводяться користувачем, можуть містити розмітку HTML – перевіряти цю розмітку за допомогою призначеної для цього бібліотеки;
- впровадити Content Security Policy.

SQL-ін'єкції стали поширеною проблемою веб-сайтів, керованих базами

даних. Вразливість легко виявити і легко використати, і будь-який веб-сайт чи додаток із навіть мінімальною базою користувачів, ймовірно, буде підданий спробі такого нападу [2]. Успішна SQL-ін'єкція може дозволити:

- отримати несанкціонований доступ до конфіденційних даних (логіни, паролі, дані кредитних карток, особисті дані користувачів);
- змінити дані в базі – підробити, закодувати, додати до них власні дані (наприклад, код для XSS-атаки);
- обмежити доступ до даних;
- знищити дані;
- створити бекдор у системі;
- змінити логіку програми.

Серйозність SQL-ін'єкцій обмежується майстерністю та уявою злоумисника та (меншою мірою) рівнем розробленого захисту. Загалом, ці атаки мають високий рівень небезпеки.

Висновки. Потенційно вразливим до атак цього виду є будь-який веб-сайт чи додаток, що використовує бази даних на мові SQL. Запобігти успішній реалізації SQL-ін'єкцій можна використовуючи наступні методи:

- використовувати підготовлені вирази (з параметризованими даними) при генеруванні запитів до бази даних. Спеціально призначені для цього методи існують на Java, .NET, PHP, Hibernate;
- використовувати збережені процедури (цей варіант у деяких випадках може замінити попередній, але є менш пріоритетним);
- Перевіряти дані, введені користувачем, по білому списку (Whitelist Input Validation) перед формуванням запиту на основі цих даних;
- Використовувати принципи мінімізації привілеїв (кожен користувач баз даних повинен мати лише мінімальні необхідні йому права, не дозволяти всім записам мати повні права адміністратора), та створювати різних користувачів для різних додатків та баз даних (уникати використання одного і того ж облікового запису власника/адміністратора) [3].

Література

1. Cross Site Scripting Prevention Cheat Sheet [Електронний ресурс]. Режим доступу: https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html.
2. SQL Injection [Електронний ресурс]. Режим доступу: https://owasp.org/www-community/attacks/SQL_Injection.
3. SQL Injection Prevention Cheat Sheet [Електронний ресурс]. Режим доступу: https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html.

АНАЛІЗ СПОСОБІВ ПОБУДОВИ ТА ФУНКЦІОНУВАННЯ СЕНСОРНИХ РАДІОМЕРЕЖ ІЗ ВИКОРИСТАННЯМ SDN

Лисенко О.І., Роспутній В.В.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: rosputnyv@gmail.com

ANALYSIS OF THE WAYS OF SDN-BASED WIRELESS SENSOR NETWORKS CREATION AND OPERATION

The article describes the technology of creation and operation SDN-based Software-Defined Wireless Sensor Networks. It shows the main advantages of using SDN for WSN and how using SDN-based wireless sensor networks solves their main disadvantages.

В даній роботі описано технологію створення та експлуатації бездротових сенсорних мереж, що визначаються програмним забезпеченням на основі SDN.

Сенсорні радіомережі (Wireless Sensor Network) - розподілені бездротові мережі, що складаються з маленьких вузлів (сенсорів), з інтегрованими функціями моніторингу навколишнього середовища, обробки і передачі даних (див. рис.1) [1, 2, 3].

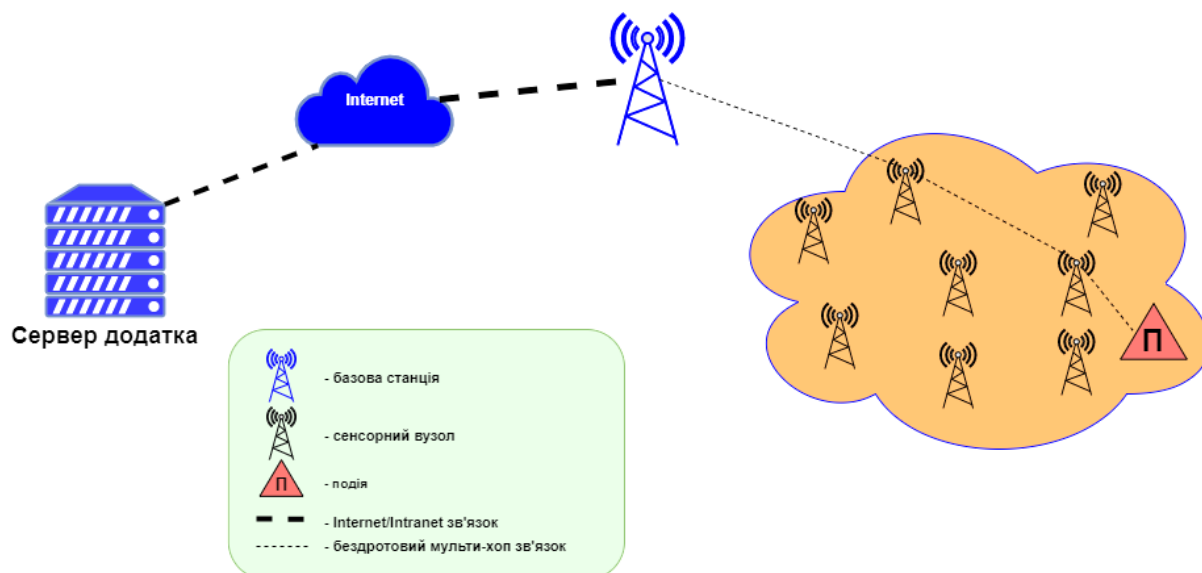


Рис. 1. Схема бездротової сенсорної мережі.

Програмно-конфігурована мережа (SDN від англ. Software-defined Networking) - це підхід, при якому для направлення трафіка в мережі та взаємодії з базовою апаратною інфраструктурою використовуються

контролери на базі програмного забезпечення або API-інтерфейси (див. рис. 2). Мережа побудована за таким підходом відрізняється від традиційних тим, що в традиційних використовуються комутатори та маршрутизатори для керування трафіком.

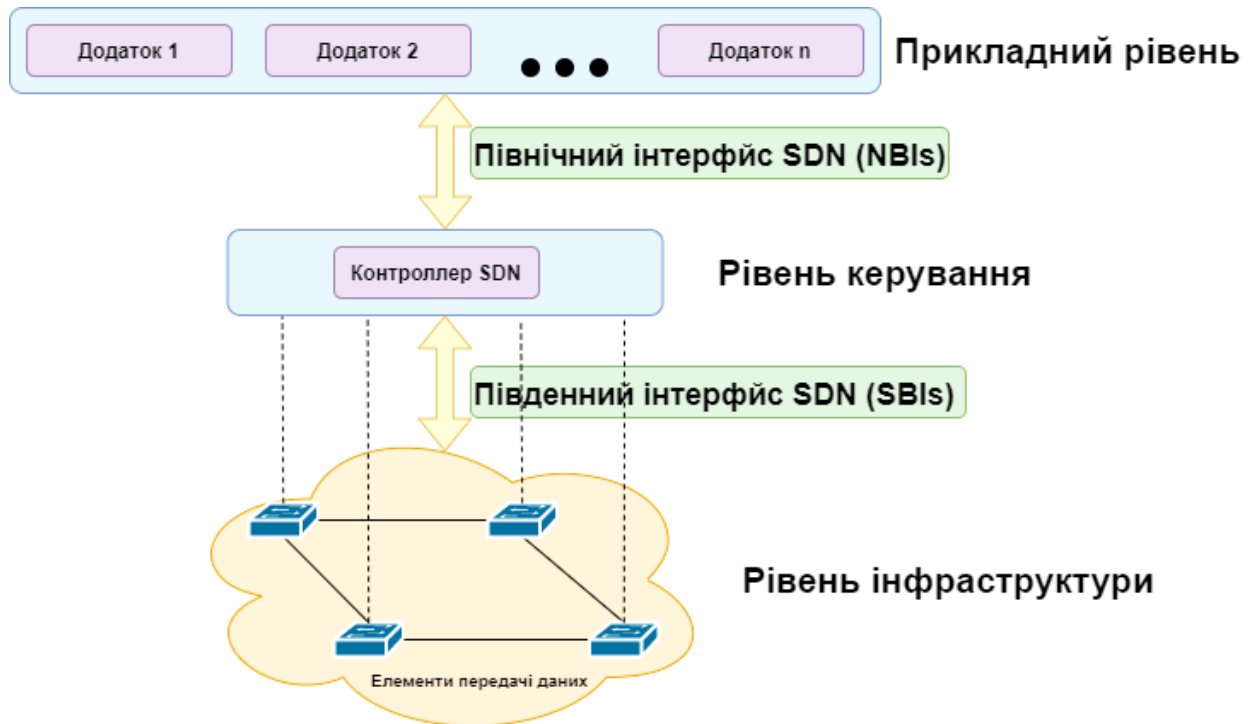


Рис. 2. Архітектура програмно-конфігурованої мережі.

Головною проблемою є те, що мережі традиційної архітектури є пропрієтарними та закритими для досліджень. Обладнання різних виробників дуже часто погано об'єднуються в одну мережу по причині того, що зазвичай кожен вендор використовує своє унікальне програмне забезпечення.

Сенсорна мережа складається з датчиків, котрі мають комунікаційні, обчислювальні та сенсорні можливості. У вузлах датчиків зазвичай є акумуляторні батареї, які обмежують час роботи кожного окремого сенсору, що також є величезною проблемою, котру необхідно вирішити.

Також варто зазначити, що датчики часто випадково розташовуються на більшій території для моніторингу ніж передбачено. Через це виникає ще одна проблема бездротових сенсорних мереж: необхідність контролювання діапазонів зв'язку та зондування для забезпечення зв'язку з іншими вузлами мережі та охоплення всієї бажаної області відслідковування.

Для вирішення вказаних проблем, були запропоновані програмно-конфігуровані сенсорні радіомережі (рис. 3), котрі дозволяють спростити роботу, взаємодію та керування сенсорними вузлами. В свою чергу це дозволить зменшити енергоспоживання вузлів датчиків, а також, полегшити управління через потужний контролер, який дасть змогу керувати всією мережею, а не лише деякими її частинами, які використовують розподілені протоколи управління. Контролер здатний управляти мережею та програмами, заощаджуючи енергію і навмисно врівноважувати залишкову енергію мережі, щоб максимально збільшити її час роботи.

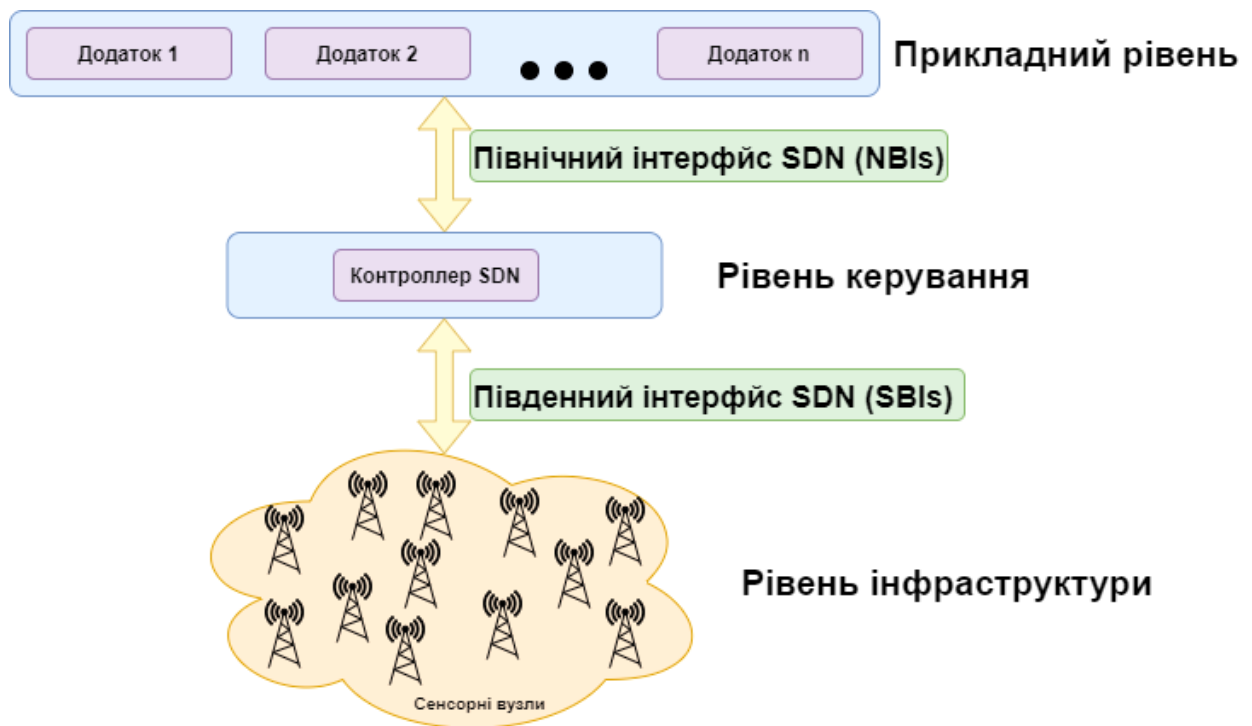


Рис.3. Архітектура сенсорної радіомережі із використанням SDN.

Висновки. В даній статті показано основні переваги використання SDN для WSN і те, як використання бездротових сенсорних мереж на основі SDN вирішує їх основні недоліки.

Література

1. Жук О.В., Міночкін А.І., Романюк В.А. Перспективи розвитку тактичних сенсорних мереж // Збірник наукових праць № 2. – К.: ВІТІ НТУУ "КПІ". – 2007. – С. 111 – 119.
2. Habib Mostafaei, Michael Menth, Software-Defined Wireless Sensor Networks: A Survey, 2018.
3. Musa Ndiaye, Gerhard P. Hancke, Adnan M. Abu-Mahfouz, Software Defined Networking for Improved Wireless Sensor Network Management: A Survey, 2017.

МЕТОД ПІДВИЩЕННЯ ЗВ'ЯЗНОСТІ МЕРЕЖ MANET ІЗ ВИКОРИСТАННЯМ БПЛА

Валуйський С.В., Турчин Я.В.

Інститут телекомунікаційних систем КІП ім. Ігоря Сікорського, Україна

E-mail: turchyn_v@ukr.net

METHOD OF INCREASING MANET CONNECTIVITY USING UAVs

This article describes the problem of maintaining connectivity between ground-based MANET nodes using multiple UAVs, which combines the problem of deploying new added UAVs and the problem of motion control of existing UAVs. The importance of considering existing UAVs to reduce the number of new UAVs added is demonstrated.

З метою вдоволення потреб сучасного суспільства, яке бажає завжди залишатися на зв'язку, а також в результаті появи на ринку різноманітних гаджетів і мобільних пристроїв, що призводять до ще більшого зростання запитів, в даний час можна спостерігати високі темпи розвитку технологій бездротової передачі даних. У свою чергу, це веде не тільки до вдосконалення вже існуючих моделей мереж зв'язку, але також і до пошуку нових варіантів застосування бездротових технологій.

Безпілотні літальні апарати (БПЛА) стали перспективними ретрансляційними платформами для поліпшення мережевих характеристик (таких як зв'язність та пропускна здатність) для наземних мобільних епізодичних радіомереж (MANET) [1]. MANET (Mobile Ad-hoc Network) – бездротова, децентралізована, мобільна IP-мережа, що здатна до самоорганізації та забезпечує встановлення з'єднань між довільними вузлами.

БПЛА мають кілька унікальних характеристик, придатних для ретрансляції:

По-перше, гнучкість руху БПЛА може розширити сферу застосування наземних мереж, особливо в сценаріях з перешкодами.

По-друге, БПЛА можуть взаємодіяти з наземними вузлами в прямій видимості, що може поліпшити пропускну здатність між наземними вузлами.

По-третє, і останнє, але не менш важливе: БПЛА, які обладнані системами зв'язку, обчислення та управління та різними датчиками, можуть виконувати моніторинг навколишнього середовища та адаптивно керувати своїм рухом. Здатність до адаптації свого положення БПЛА робить їх придатними для надання ретрансляційних послуг для MANET, що мають динамічну топологію мережі.

На сьогодні було докладено багато зусиль для вивчення переваг використання БПЛА в якості ретрансляторів зв'язку для наземних MANET. Однак існуючі роботи з розгортання БПЛА не враховували ситуацію, коли деякі БПЛА вже були розгорнуті на місцях [2]. Під час руху наземних MANET існуючі БПЛА можуть не зуміти з'єднати всі наземні вузли. В такому випадку потрібно вивести нові БПЛА для підтримки зв'язності

наземних абонентів. Для того, щоб мінімізувати кількість нових доданих БПЛА, слід враховувати переміщення як існуючих, так і розміщення нових БПЛА. Це спільна проблема оптимізації, яка оптимізує як розгортання, так і управління рухом кількох БПЛА. В [3] розглядається можливість використання існуючих БПЛА, переміщуючи їх у належні положення, таким чином зменшуючи кількість необхідних нових БПЛА. Існуючі БПЛА мають обмежений діапазон руху, який залежить від швидкості БПЛА.

Для підтримки двоспрямованого зв'язку між БПЛА та наземними вузлами ми припускаємо, що БПЛА мають такий самий діапазон зв'язку, як і наземні вузли. На рис. 1 показаний приклад того, як контроль руху існуючих БПЛА може зменшити кількість необхідних нових БПЛА. Припустимо, що в полі розгорнуто два наземних вузли та два існуючі БПЛА. Оскільки відстань між двома наземними вузлами більше, ніж їхній діапазон зв'язку r , наземна мережа MANET розділена на дві частини, що показано на рис.1(а).

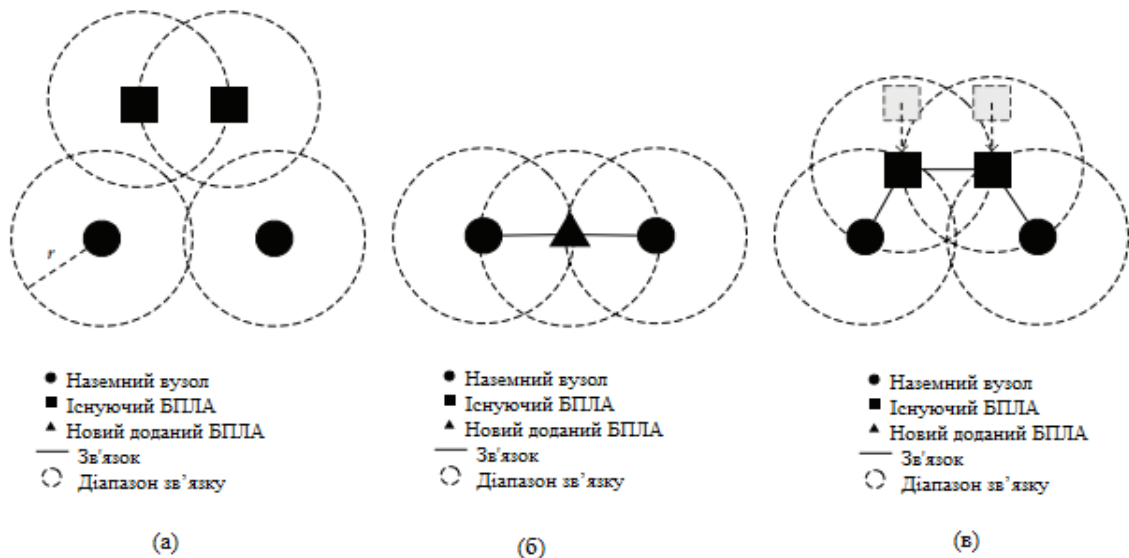


Рис.1. Приклад, який ілюструє важливість існуючих БПЛА у підтримці зв'язку наземних MANET.

Для того, щоб підтримувати зв'язок наземних MANET, методи, які не враховують існуючі БПЛА, додадуть нові БПЛА для з'єднання розділених частин, як показано на рис.1(б). Тут новий БПЛА додано і розміщено посередині двох наземних вузлів. Тож ці два наземні вузли тепер можуть комунікувати між собою за допомогою нового БПЛА. Не розглядаючи існуючі БПЛА, потрібно розгорнути принаймні один додатковий БПЛА, щоб підтримувати зв'язок наземних абонентів [4].

Щоб зменшити капітальні витрати, користувачі намагатимуться всіма силами зменшити кількість нещодавно розгорнутих БПЛА. Іншими словами, вони будуть використовувати наявні БПЛА, а не ігнорувати їх. Переміщаючи існуючі БПЛА у належні положення та використовуючи існуючі БПЛА як ретранслятори, можна покращити зв'язок наземних абонентів [5].

На рис.1(в) показано траєкторію руху існуючих БПЛА. Їх треба

перемістити безпосередньо до границі діапазону наземних вузлів, таким чином щоб відстань між існуючими БПЛА і одним наземним вузлом була меншою за дальність зв'язку r . Після цього між двома наземними вузлами встановлюється маршрут передачі даних із ретрансляцією через існуючі БПЛА. Таким чином, підтримується зв'язок наземних абонентів MANET, і розгортання нових БПЛА не потрібно [6].

Для того, щоб вирішити спільну проблему оптимізації розгортання та управління рухом декількох БПЛА, щоб кількість нових доданих БПЛА була мінімізована, спочатку треба сформулювати цю проблему як проблему мінімального дерева Штейнера з існуючими мобільними точками Штейнера та ребрами обмеженої довжини (MST-EMSELB) і довести NP повноту проблеми. Потім представити алгоритм розміщення неіснуючих БПЛА та розглянути три алгоритми апроксимації поліноміального часу розміщення існуючих БПЛА:

- Розгортання-перед-переміщенням (Deploy-Before-Movement, DBM);
- Переміщення-перед-розгортанням (Move-Before-Deployment, MBD);
- Розгортання-під час-переміщення (Deploy-Across-Movement, DAM).

Перші два алгоритми розділяють загальну проблему на проблему розгортання нових БПЛА та задачу управління рухом існуючих БПЛА. Алгоритм DBM оптимізує розгортання нових БПЛА перед переміщенням існуючих БПЛА, а алгоритм MBD вирішує проблему протилежним чином. Алгоритм DAM – це змішаний алгоритм, який вирішує проблему переміщення та розгортання одночасно. Симуляційні експерименти показують, що всі алгоритми розміщення існуючих БПЛА мають кращі показники щодо числа нових БПЛА, ніж алгоритми розміщення неіснуючих БПЛА. Алгоритм DAM завжди кращий за алгоритми DBM та MBD і може підвищити продуктивність максимум до 70% порівняно з алгоритмом DBM.

Література

1. Z. Han, A. L. Swindlehurst, and K. J. R. Liu, "Optimization of MANET connectivity via smart deployment/movement of unmanned air vehicles," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 7, pp. 3533–3546, 2009.
2. K. Chandrashekar, M. R. Dekhordi, and J. S. Baras, "Providing full connectivity in large ad-hoc networks by dynamic placement of aerial platforms," in *Proceedings of the IEEE Military Communications Conference (MILCOM '04)*, vol. 3, pp. 1429–1436, IEEE, Monterey, Calif, USA, October-November 2004.
3. F. Jiang and A. L. Swindlehurst, "Optimization of UAV heading for the ground-to-air uplink," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 5, pp. 993–1005, 2012.
4. C. Dixon and E. W. Frew, "Optimizing cascaded chains of unmanned aircraft acting as communication relays," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 5, pp. 883–898, 2012.
5. E. L. Lloyd and G. Xue, "Relay node placement in wireless sensor networks," *IEEE Transactions on Computers*, vol. 56, no. 1, pp. 134–138, 2007.
6. W. Zhang, G. Xue, and S. Misra, "Fault-tolerant relay node placement in wireless sensor networks: problems and algorithms," in *Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM '07)*, pp. 1649–1657, IEEE, Anchorage, Alaska, USA, May 2007.

МЕТОД ПРОЕКТУВАННЯ РОЗМІЩЕННЯ ДАТЧИКІВ БЕЗДРОТОВОЇ СЕНСОРНОЇ МЕРЕЖІ

¹Гордійко Н.О., ²Томашевська Т.В.

¹*Фізико-технічний інститут КІІ ім. Ігоря Сікорського, Україна*

²*Національна академія статистики, обліку та аудиту, Україна*

E-mail: natalygor22@gmail.com; tomas_tat@ukr.net

METHOD OF DESIGN OF LOCATION OF SENSORS OF THE WIRELESS SENSOR NETWORK

The article describes approaches to determining the optimal coverage of sensors in the sensor network based on the solution of the problem of finding the local optimum distribution of sensing areas.

В доповіді пропонується підхід для визначення розміщення датчиків сенсорної мережі як рішення задачі оптимального покриття за допомогою наближеного методу пошуку локального оптимуму.

Служба моніторингу стану довкілля потребує отримання своєчасної та точної інформації, яка б могла забезпечити оперативне реагування у випадках надзвичайних ситуацій, оскільки їх розвиток може призвести до втрат цінних природних ресурсів та загроз життю та майну. Так, з метою уникнення значних витрат на ліквідацію наслідків, визначення потенційного забруднення ґрунтів потребує якомога більш раннього проведення.

Останні технологічні досягнення призвели до розвитку бездротових мережевих технологій, які можна використовувати для вирішення зазначених вище проблем.

Бездротові сенсорні мережі складаються з сукупності датчиків, що мають можливість повідомляти або реагувати на події всередині їх поля зондування. Відповідно до характеру проблем, для яких використовуються датчики, типи пристроїв, що входять до загального датчика, розрізняються за своїм складом.

Хоча кожен датчик може вимірювати характеристики середовища (наприклад, температуру, вологість, концентрацію забруднення тощо) у певному місці, за допомогою мережі розподілених спостережень фізичне поле певної характеристики може бути реконструйовано шляхом розв'язання оберненої задачі [1].

На оцінку фізичного поля суттєво впливає кількість вузлів датчиків та їх просторове розташування, що тісно пов'язано з покриттям, вартістю сенсорів, споживанням енергії. Тому визначення найменшої кількості необхідних вузлів датчиків та їх розміщення є основним питанням при проектуванні сенсорної мережі [2].

Отже, проблема побудови поля фізичної характеристики певного явища полягає у пошуку найменшої кількості необхідних датчиків, що

забезпечують зондування області з точністю, відповідною заданим вимогам. Тобто необхідно розв'язати оптимізаційну задачу наступного виду:

$$\min_k S(k) \text{ при } \mu(U_{S(k)}) < \varepsilon, \quad (1)$$

де k – кількість датчиків;

$S(k)$ – певна конфігурація розподілу k датчиків;

U_k – реконструйоване значення фізичного поля на основі даних k датчиків;

$\mu(X)$ – функція близькості, яка визначається як відстань в просторі характеристики;

ε – задана точність.

Дана задача є задачею про покриття з обмеженнями. Очевидно, що прямий метод розв'язання такої задачі полягає в оцінці ефективності всіх можливих комбінацій різної кількості датчиків з наступним вибором множини з найменшим числом вузлів датчиків, що задовольняє необхідній точності оцінки. Але, враховуючи, що алгоритм про покриття належить до NP-складних задач, такий підхід неможливо реалізувати, якщо потенційна кількість датчиків є великою [2].

На сьогодні сформувалися два принципово різних підходи до розв'язання NP-повних задач: або оптимізувати не поліноміальний метод розв'язання або, у випадках, коли це доречно, обмежитися пошуком наближеного розв'язку.

Існує велика кількість методів побудови алгоритмів для розв'язання NP-повних задач. Основними з них є [3-4]:

- наближені й евристичні методи – застосування евристик для вибору елементів розв'язку;
- псевдополіноміальні алгоритми – підклас динамічного програмування;
- метод локальних поліпшень – пошук більш оптимального розв'язку в околі деякого поточного розв'язку;
- метод гілок і меж – відкидання свідомо неоптимальних розв'язків цілими класами відповідно до деякої оцінки;
- метод випадкового пошуку – представлення вибору послідовністю кількох випадкових виборів.

Визначення покриття сенсорних датчиків також залежить від моделі покриття, що використовується для кожного датчика. Загальноприйнятим є припущення, що кожна область зондування для датчика є ізотропною областю (в двовимірному просторі – коло, в тривимірному просторі – сфера). Доволі часто це припущення не відповідає дійсності та суттєво залежить від типу датчиків, типу області моніторингу. Особливості задачі моніторингу навколишнього середовища можуть потребувати нерівномірного розташування датчиків – збільшення кількості датчиків в одній частині області та їх розрідження в інших частинах.

Виходячи з наведених умов, пропонується використовувати опуклі

неправильні п'ятикутники, що вкривають площину без розривів та перетинів. Крім того, їх використання дає змогу ущільнювати або навпаки розріджувати кількість датчиків розбиття в області моніторингу, збільшуючи або зменшуючи розміри п'ятикутників без зміни загальної форми області [5,6].

Для визначення близькості між точками пропонується використовувати функцію вигляду

$$\mu(X) = \sum_{i=1}^K \sum_{j=1}^d u_{ij}^w d^2(X_j, X_i). \quad (2)$$

Функцію відстані визначаємо таким чином:

$$d^2(X_j, X_i) = \|X_j - X_i\|^2 = (X_j - X_i)^T (X_j - X_i). \quad (3)$$

Параметр u_{ij}^w визначається як властивість датчиків охоплювати зондуванням відповідну територію з коефіцієнтом впевненості w (зазвичай, дорівнює 2)

$$u_{ij}^w = \frac{1}{\sum_{j=1}^k \sum_{i=1}^k \left(\frac{d^2(X_j, X_i)}{d^2(X_j, X_i)} \right)^{\frac{1}{w-1}}}. \quad (4)$$

Після вибору першого наближення відбувається пошук локального оптимуму задачі (1) на основі запропонованих функцій (2) - (4).

На основі наведеного підходу можна побудувати алгоритм визначення оптимального покриття сенсорною мережею довільної області. Такий алгоритм є актуальним при виборі геометричної конфігурації сенсорної мережі.

Література

1. V. Akbarzadeh, J.-C. Lévesque, C. Gagné and M. Parizeau, "Efficient Sensor Placement Optimization Using Gradient Descent and Probabilistic Coverage", *Sensors* 2014, 14, 15525-15552; doi:10.3390/s140815525.
2. C. Jiang, Y. C. Soh, and H. Li, "Sensor placement by maximal projection on minimum eigenspace for linear inverse problems", arXiv:1506.00747v3 [cs.DS] 5 Nov 2016.
3. Кормен, Т., Лейзерсон, Ч., Ривест, Р., Штайн, К. Алгоритмы: построение и анализ – Introduction to Algorithms /Под ред. И. В. Красикова. Млсква : Вильямс, 2005. 1296 с.
4. Ахо А., Хопкровт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов, Москва: Мир, 1979. 536 с.
5. Гордійко Н.О., Лисенко О.І., Томашевська Т.В. Застосування методу використання геометричних фракталів для оптимального розміщення сенсорів при екологічному моніторингу / Н.О. Гордійко, О.І. Лисенко, Т.В. Томашевська. Зб. матеріалів XI Міжнар. наук.-тех. конференції «Проблеми телекомунікацій» ПТ-2017, (м.Київ, 18–21 квітня 2017), с.392-394.
6. Застосування п'ятикутного покриття для визначення оптимального розташування сенсорів у задачах екологічного моніторингу // Наукові праці Другої міжнар. наук.-практ. конф. «Сучасні тенденції розвитку інформаційних систем і телекомунікаційних технологій», 19 грудня 2019 р. (Київ, Україна), 2019. – С.32-34.

МОДЕЛЮВАННЯ ПАРАМЕТРІВ РУХУ МАНЕВРУЮЧИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ НА ОСНОВІ СТІЙКОГО АЛГОРИТМУ ДИНАМІЧНОЇ ФІЛЬТРАЦІЇ

Якорнов Є.А., Цуканов О.Ф.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: cukanov-o@ukr.net

MODELING THE MOTION PARAMETERS OF MANEUVERING UNMANNED AERIAL VEHICLES BASED ON A STABLE DYNAMIC FILTERING ALGORITHM

The results of modeling the parameters of movement of maneuvering unmanned aerial vehicles using an estimation algorithm, in which stability is ensured by estimating coordinates and their derivatives, are considered.

В роботі [1] авторами запропоновано стійкий алгоритм оцінки параметрів руху маневрують безпілотних літальних апаратів (БПЛА) як елементів літаючих бездротових систем, що самоорганізуються сенсорних мереж в якому стійкість забезпечується шляхом оцінки координат і їх похідних на основі фільтра Калмана [2] в припущенні, що помилки визначення координат мають закон розподілу помилок, який в загальному випадку відрізняється від нормального. У цьому випадку використання модифікованого алгоритму динамічного оцінювання на основі фільтра Калмана дозволяє, на наш погляд, отримати як усталені оцінки БПЛА, так і забезпечити їх високу точність.

Нижче наведені деякі результати моделювання запропонованого в [1] алгоритму, суть якого полягає в наступному:

- 1) оцінка вектору стану (ВС) у вигляді координат і параметрів руху (швидкості, а деяких випадках і прискорення БПЛА), точність оцінювання якого визначаються шляхом вимірювання відстаней між БПЛА;
- 2) оцінка кореляційної матриці помилок (КМО) ВС, яка для кожного БПЛА мережі залежить від багатьох факторів, основними з яких є помилки визначення координат БПЛА;
- 3) екстраполяція ВС шляхом його подання у вигляді складання матриць екстраполяції і управління;
- 4) введення до вектору управління параметру стійкості процесу оцінювання γ , який забезпечує «примусове збільшення» значень діагональних елементів матриці управління [2];
- 5) задавання моделі руху БПЛА.

Математичне подання цього алгоритму приведено в доповіді, а для моделі руху БПЛА обрана модель, заснована на реальних технічних

характеристиках БПЛА «Орлан» [3], яка описується алгебраїчним багаточленом 5-го ступеню за координатами:

$$\hat{Z}_t = a_0 + a_1 t_{i-1} + a_2 t_{i-1}^2 / 2 + a_3 t_{i-1}^3 / 6 + a_4 t_{i-1}^4 / 24 + a_5 t_{i-1}^5 / 120, \quad (1)$$

поліномом 4-го ступеню за швидкостями:

$$\tilde{Z}_t = a_1 + a_2 t_{i-1} + a_3 t_{i-1}^2 / 2 + a_4 t_{i-1}^3 / 6 + a_5 t_{i-1}^4 / 24 \quad (2)$$

та поліномом 3-го ступеню від прискорення:

$$\tilde{\tilde{Z}}_t = a_2 + a_3 t_{i-2} + a_4 t_{i-2}^2 + a_5 t_{i-2}^3 / 6. \quad (3)$$

Стійкість оцінки ВС БПЛА забезпечується множенням на параметр γ . Ця операція, в свою чергу, призводить до нижньої межі значень елементів матриці посилення динамічного фільтру. Таким чином, постійними в алгоритмі є параметр γ й величина Δt (час між вимірами відстані між БПЛА). У зв'язку з цим при моделюванні можна попередньо задати елементи вектору управління КМО для забезпечення стійкості та необхідної точності оцінки.

Наведемо деякі результати моделювання. Зокрема, моделювався політ БПЛА при його прямолінійному русі та наступних типів маневру: відходу від лобового зіткнення, набір висоти і плавний розворот на 90° з подальшим переходом до прямолінійного руху (див. Рис. 1 при $\gamma = 0$ та Рис. 2 при $\gamma = 0,4$ за координатами і похідним).

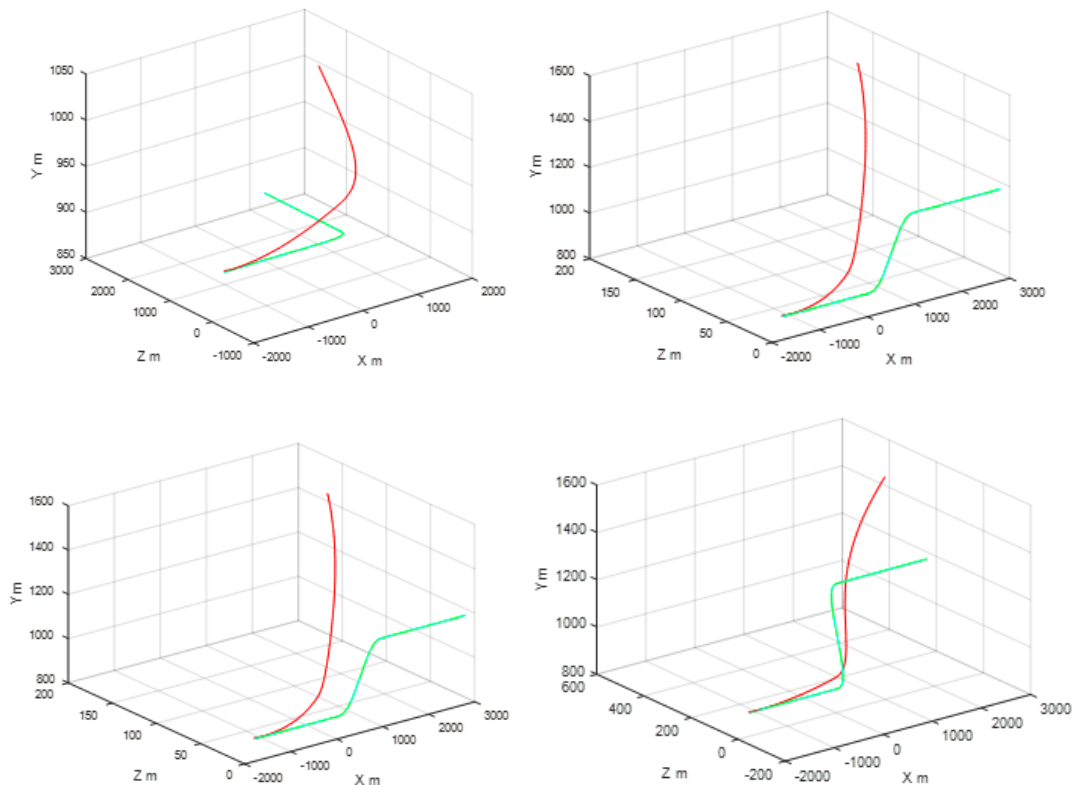


Рис. 1. Результати моделювання.

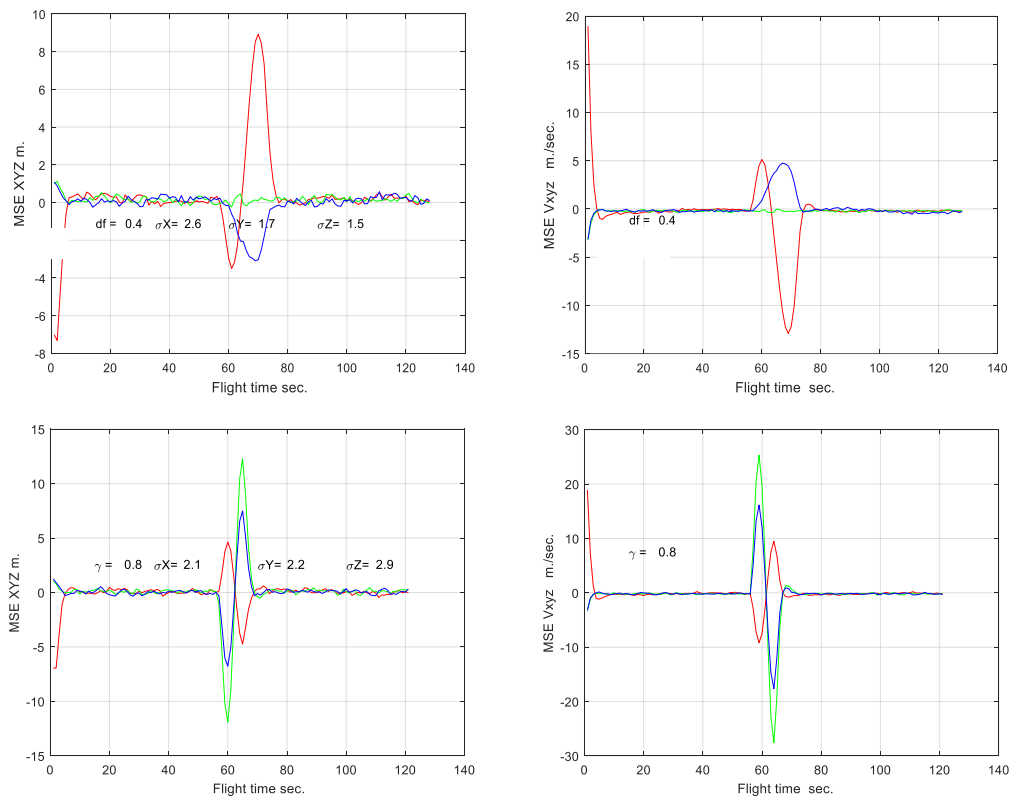


Рис. 2. Результати моделювання.

Крім того, було проведено аналіз величини похибки оцінки за координатами та швидкості, розподілених на 100 реалізацій. При прямолінійному русі максимальна похибка визначення координат становить 4,5 м - $\gamma = 0,1$, мінімальне 1,6 м - $\gamma = 0,8$. На ділянці маневру: максимальна похибка за координатами 18 м - $\gamma = 0,1$, мінімальне 5 м - $\gamma = 0,4$, максимальна похибка швидкості 18 м/с - $\gamma = 0,1$, мінімальне 10 м/с - $\gamma = 0,8$.

Результати моделювання дозволяють припустити, що запропонований стійкий алгоритм оцінки відстаней між БПЛА з багаторазовими вимірами дозволяє отримувати стійкі оцінки координат ВС і їх похідних і одночасно підвищується точність визначення координат БПЛА.

Література

1. O. Tsukanov, E. Yakornov Estimation of the motion parameters of the UAVs FANET using the dynamic filtering method. Springer Nature Switzerland AG 2019 M. Ilchenko et al. (Eds.): UKRMICO 2018, LNEE 560, pp. 239–261, 2019. https://doi.org/10.1007/978-3-030-16770-7_12C. 303-318.
2. Grewal M.S., Andrews A.P., "Kalman Filtering – Theory and Practice Using MATLAB", Wiley, 2001.
3. Мельник Н.О. Полная математическая модель беспилотного летательного аппарата в условиях движения с мешающими воздействиями. // Вестник Воронежского государственного технического университета. 2015, Volume: 11, No. 2, pp. 31-33, ISSN: 1729-6501.

РОБАСТНОСТНИЙ ПІДХІД ДО ЗАДАЧІ ПІДВИЩЕННЯ ТОЧНОСТІ ВИЗНАЧЕННЯ КООРДИНАТ ЕЛЕМЕНТІВ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

Якорнов Є.А., Цуканов О.Ф.

Інститут телекомунікаційних систем КІП ім. Ігоря Сікорського, Україна

E-mail: cukanov-o@ukr.net

ROBUST APPROACH TO THE PROBLEM OF INCREASING THE ACCURACY OF DETERMINING THE COORDINATES OF ELEMENTS OF WIRELESS SENSOR NETWORKS

A robust approach to solving the problem of increasing the accuracy of determining coordinates of elements of wireless sensor networks for the case of a difference in the distribution law of measurement errors from the normal one and some simulation results are given.

Бездротові сенсорні мережі (БСМ) знаходять все більше застосувань, особливо при розгортанні сенсорів в зонах надзвичайних ситуацій (НС), та при їх вдосконаленні, як і раніше, багато уваги приділяється питанням збору інформації, енергетичної ефективності й маршрутизації, а також підвищенню точності визначення координат вузлів БСМ [1, 2].

Розглянемо наступну постановку задачі. Є БСМ, яка складається з n нерухомих, після розгортання в зоні НС або переміщення, елементів. Координати елементів БСМ визначаються шляхом вимірювання взаємних відстаней. Прийmemo, що похибки вимірювань розподілені за законом, який близький до нормального. Необхідно підвищити точність визначення координат сенсору при законі розподілу помилок вимірювань відмінному від нормального, що має місце через складне нелінійне перетворення. Останнє призводить до того, що координати сенсору будуть визначатися шляхом усереднення, при якому оцінка координат не буде незсуненою, консистентною та ефективною.

Для усунення цього недоліку при оцінюванні координат сенсорів розглянемо можливості використання робастних методів оцінювання [3, 4]. Наприклад, при невідомому законі розподілу похибок вимірювань взаємних відстаней можливе використання мінімаксий підхід Хьюбера [3]. Тоді, в якості оцінки координат береться така, яка буде мати похибку мінімальну з максимально можливих. Зауважимо, що в разі симетричності закону розподілу робастна оцінка Хьюбера стає нестійкою. Тоді найбільш робастною (стійкою до закону розподілу похибок) є медіанна оцінка. А при вирішенні завдання підвищення точності визначення координат місця розташування сенсорів БСМ - використання функцій впливу [3, 4], які показують який вплив на оцінку має аномальне вимір, та наскільки від його «страждає» точність одержуваної оцінки.

Суть підходу на основі використання функції впливу Хьюбера полягає в припущенні, що в реальній вибірці, похибки вимірювань розподілені за двома законами розподілу. Перший основний $N(x, D_1)$ - нормальний закон розподілу з нульовим середнім і дисперсією похибок вимірювань D_1 , другий - $R(x, D_2)$, нормальний закон розподілу з нульовим середнім і дисперсією похибок вимірювань D_2 .

Результуючий закон розподілу с «забрудненням» має вигляд:

$$P(x) = (1 - \varepsilon)N(x, D_1) + \varepsilon R(x, D_2), \quad (1)$$

де ε – параметр забруднення, який на практиці береться таким, що дорівнює 0,05 - 0,1.

При $\varepsilon \rightarrow 0$, в якості оцінки приймається арифметичне середнє, в разі $\varepsilon \rightarrow 1$ - медіана вибірки.

Вихідними даними для моделювання, є еталонні значення координат двох сенсорів: (X_{e1}, Y_{e1}) , (X_{e2}, Y_{e2}) на основі яких визначається оцінка координат чергового сенсору (позначимо їх як $(X_{e3}$ та $Y_{e3})$). Оцінка проводилася за допомогою методу Ньютона-Рафсона [3]:

$$X_{k+1} = X_k + W_k^{-1} f_k, \quad (2)$$

де f_k - вектор вимірюваних дальностей r_{1k}, r_{2k} до k -го сенсору;

W_k^{-1} - матриця часткових похідних r_{1k}, r_{2k} за координатами x, y ;

X_{k+1} - шукані координати поточного сенсору.

На рис. 1 представлені результати моделювання при $n = 100$ у вигляді гістограм (синій колір) і графіків нормального закону розподілу оцінок координат (червоний колір) при еталонних значеннях $X_{e3} = 199,98$ (рис. 1.а), $Y_{e3} = 691,61$ (рис. 1.б) розподілених за нормальним законом з нульовим середнім та дисперсією $S_{D1} = 4m$.

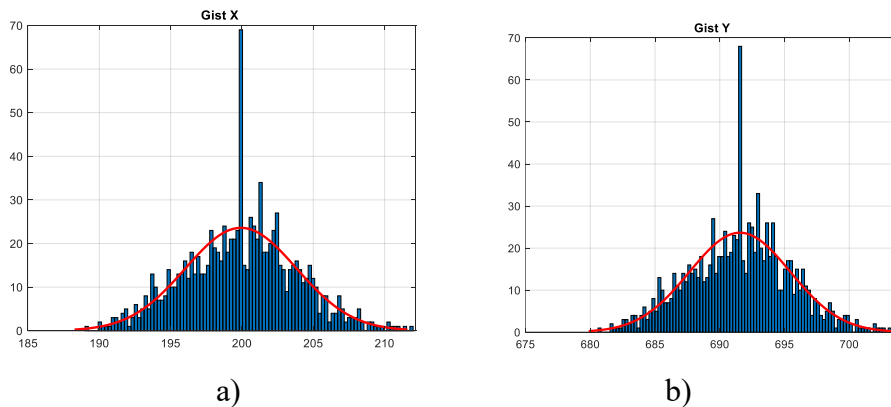


Рис. 1. Результати моделювання при $n = 100$.

Далі, на рис. 2 для тих самих еталонних значень оцінок ($X_{e3} = 199,98$, $Y = 691,61$), наведено результати моделювання з використанням робастного методу оцінювання. Для $\epsilon = 5\%$ при невеликій відмінності дисперсії основного закону розподілу $N(x, D_1)$ з дисперсією $S_{D1} = 3m$ від «забрудненого» $R(x, D_2)$ з дисперсією $S_{D2} = 4m$. У першому випадку, в якості оцінки береться медіана, а в другому оцінка з використанням функції впливу Хьюбера [3].

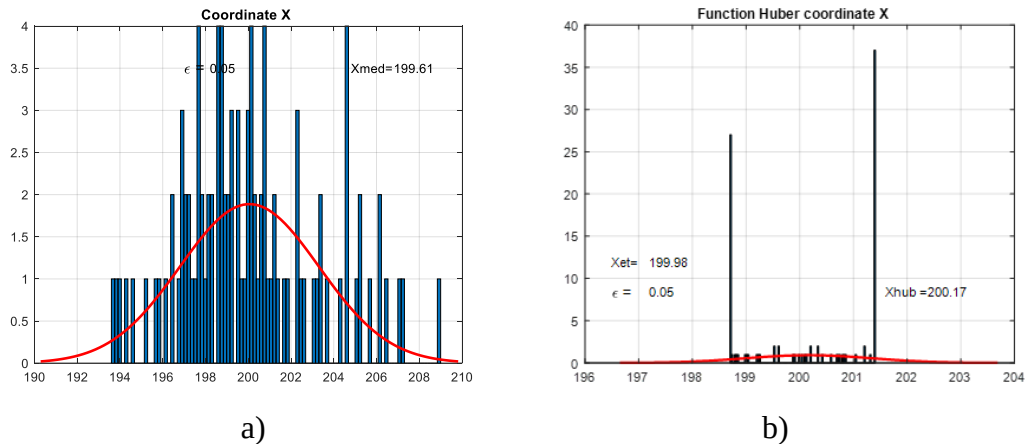


Рис. 2. Результати моделювання з використанням робастного методу оцінювання.

Аналіз гістограм на рис. 1 і 2 показує, що гістограма з використанням закону розподілу (1) (рис. 2.а) не має чітко вираженого максимуму, який до того ж не збігається із середнім значенням. Отримані оцінки з використанням функції впливу Хьюбера X_{hub} , Y_{hub} найбільш близькі до еталонних значень оцінки координат сенсорів X , Y в порівнянні з медіанною оцінкою.

Таким чином порівняння робастних методів оцінювання на основі медіанної оцінки та оцінки функції впливу показує, що останній метод оцінювання більш точний. Результати моделювання показують, що використання робастних методів оцінювання при відмінному законі розподілу похибок вимірювань від нормального, дозволяє підвищити точність визначення координат місця розташування нерухомих елементів БСС в середньому на 5-10%.

Література

1. Власова В.А. Метод определения координат объектов на этапе инициализации гомогенной беспроводной сенсорной сети: диссер. к. т. н.: 05.12.02. – Х.: ХНУРЕ, 2014.– 165 с.
2. Olexandr Lysenko, Stanislav Valuisky Secured wireless sensor network for environmental monitoring // Volume of Scientific Papers, Security forum 2016, Slovakia, Banská Bystrica, 2016, vol.2, pp. 528-532. ISBN 978-80-557-1094-5.
3. Хампель Ф. Рончетти, Э.Рауссей П.Штаэль В. Робастность в статистике. Подход на основе функции влияния. -М.Мир,1984, - 512 с.
4. Шуленин В.П. Робастные методы математической статистики. -Томск: Изд-во НТЛ, 2016-260 с.

**АНАЛІЗ ТОЧНОСНИХ ХАРАКТЕРИСТИК
КОРЕЛЯЦІЙНО-ЕКСТРЕМАЛЬНОГО АЛГОРИТМУ
СТЕЖЕННЯ ЗА МАЛОРОЗМІРНИМ БПЛА З
ВИКОРИСТАННЯМ ФІЛЬТРУ КАЛМАНА**

Жук С.Я., Герасименко А.О., Соколов К.А.

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

**ANALYSIS OF THE ACCURACY CHARACTERISTICS OF THE
CORRELATION-EXTREMAL ALGORITHM FOR TRACKING A
SMALL-SIZED UAV USING THE KALMAN FILTER**

With the help of statistical modeling, the analysis of the accuracy characteristics of the correlation-extreme algorithm for tracking a small-sized UAV using the Kalman filter was carried out and it was shown that it provides sub-pixel accuracy of the UAV position estimate at the current frame.

Шляхом статистичного моделювання проведено аналіз точносних характеристик кореляційно-екстремального алгоритму стеження за малорозмірним БПЛА з використанням фільтру Калмана і показано, що він забезпечує субпіксельну точність оцінювання положення БПЛА на поточному кадрі

В даний час малорозмірні безпілотні літальні апарати (БПЛА) знаходять все більше застосування в багатьох галузях економіки, а також для задоволення потреб комерційних і приватних споживачів. З іншого боку, їх розвиток і поширення призвели до появи нових загроз: шпигунство, тероризм, транспортування заборонених вантажів тощо. Тому важливими завданнями є відстеження БПЛА і контроль за дозволеною для них діяльністю. Важливим класом систем, які використовуються для їх вирішення є системи відеоспостереження [1]. Для реалізації супроводу рухомих об'єктів на послідовності зображень застосовується кореляційно-екстремальний метод [2,3], який має високу ефективність в силу використання не тільки характеристик яскравості об'єктів, але й їх форми та положення.

БПЛА на зображенні представляє собою сукупність зв'язаних точок. Він розміщується в прямокутній області, яка є моделлю об'єкту спостереження, і представляє еталонне зображення. Для визначення зміщення зображення БПЛА на поточному кадрі відносно еталонного зображення використовується кореляційно-екстремальний алгоритм. Стеження за БПЛА на послідовності зображень виконується з використанням фільтру Калмана [4].

Аналіз кореляційно-екстремального алгоритму стеження за малорозмірним БПЛА з використанням фільтру Калмана виконано шляхом

статистичного моделювання у середовищі Матлаб. Розмір кадру дорівнював 1080×1920 пікселів. Зображення БПЛА перетворено з формату RGB до монохромного. При цьому яскравість приведена до діапазону $[0,1]$. Моделювався рух цілі на основі поліноміальної моделі другого порядку по кожній осі в прямокутній системі координат із початковими становищем $x_1=100$ пікс (пікселів), $y_1=100$ пікс і швидкістю $\dot{x}=10$ пікс/такт, $\dot{y}=10$ пікс/такт. Інтенсивність маневру встановлено $\sigma_a=1$ пікс/такт². Кількість відліків траєкторій $N=20$. Помилки вимірювання прямокутних координат цілі кореляційно-екстремальним методом встановлено $\sigma_x=\sigma_y=1$ пікс. СКВ шуму на зображенні $\sigma_n=0,1$. Кількість реалізацій метода Монте-Карло дорівнює 100.

На рис. 1 представлені незашумлене і зашумлене еталонні зображення БПЛА розміром 10×6 пікс. На рис. 2 представлені результати обчислення нормованої взаємної кореляційної функції еталонного і поточного зображень, спотворених шумом.

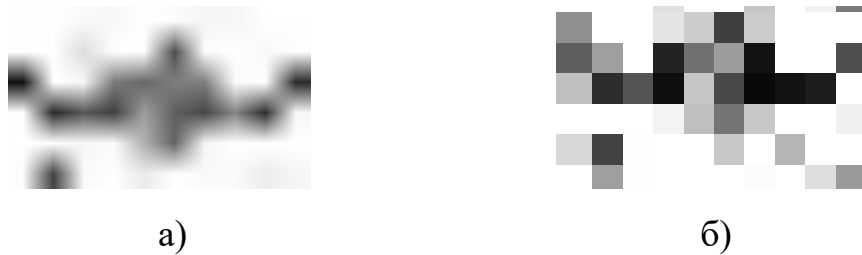


Рис. 1. Зображення еталону 10×6 пікселів а) без шуму, б) з шумом.

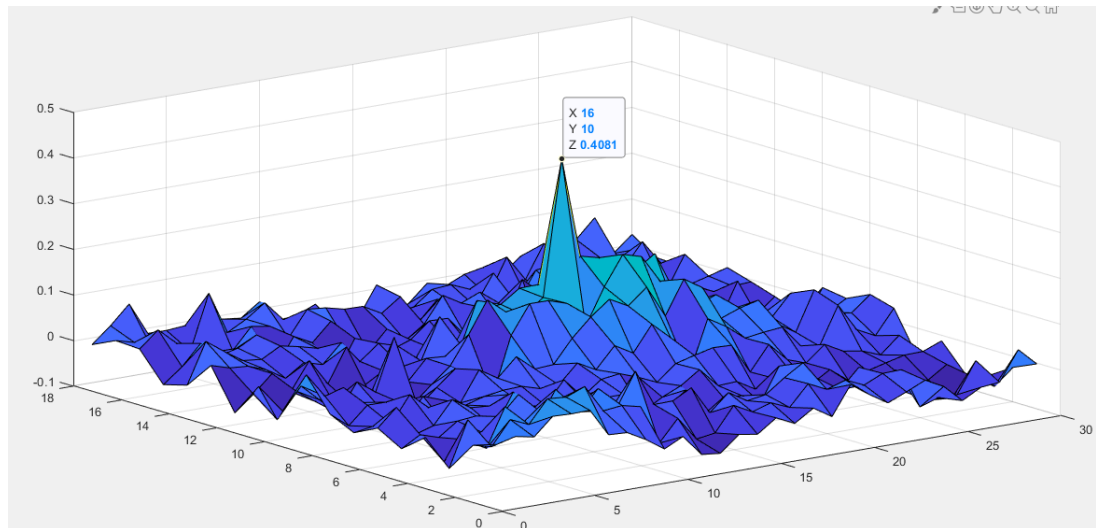


Рис. 2. Нормована взаємна кореляційні функція зашумлених зображень.

На рис.3 (а,в) показані математичні очікування m_x^*, m_y^* (зелена криві 1), СКВ помилок прогнозу положення цілі σ_x^*, σ_y^* (синя криві 2), що отримані методом Монте-Карло та СКВ помилок прогнозу положення цілі, що

розраховані фільтром $\sqrt{p_x^*}, \sqrt{p_y^*}$ (червона криві 3). На рис. 3 (б,г) показані математичні очікування $\hat{m}_x, \hat{m}_y$ (криві 1), СКВ помилок оцінки положення цілі $\hat{\sigma}_x, \hat{\sigma}_y$ (криві 2), що отримані методом Монте-Карло та СКВ помилок оцінки положення цілі, що розраховані фільтром $\sqrt{\hat{p}_x}, \sqrt{\hat{p}_y}$ (криві 3).

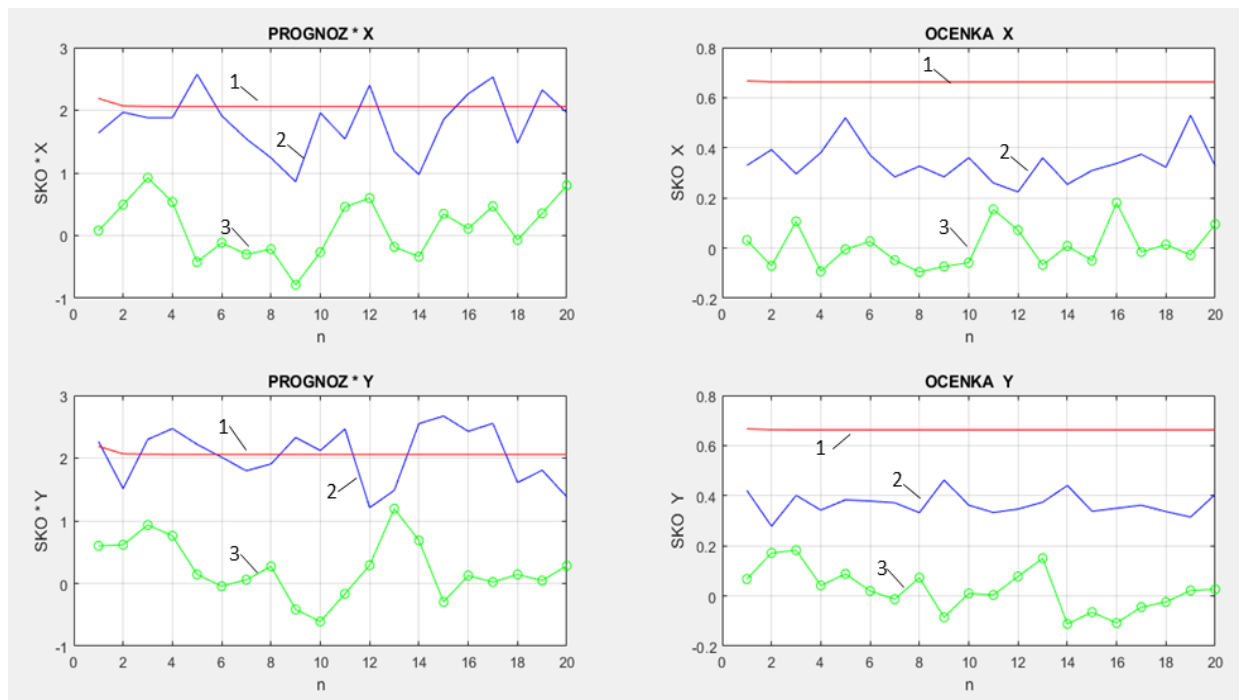


Рис. 3. Залежності математичного очікування і СКВ помилок прогнозу і оцінки координат БПЛА по осям X і Y.

Висновки. Як впливає з отриманих результатів кореляційно-екстремальний алгоритм стеження забезпечує субпіксельну точність оцінювання положення БПЛА на поточному кадрі. Він забезпечує стійке супроводження БПЛА при вхідному відношенні сигнал/шум $q > 3$ дБ. При $q < -2.7$ дБ ймовірність зриву супроводження БПЛА спрямовується до одиниці.

Література

1. Алгоритмическое обеспечение оптико-электронных систем комплекса защиты объектов от беспилотных летательных аппаратов / В. А. Бондаренко, Г. Э. Каплинский, В. А. Павлова, В. А. Тупиков. // Известия ЮФУ. Технические науки. – 2018. – С. 15–27.
2. Алпатов Б.А., Бабаян П.В., Балашов О.Е., Степашкин А.И. Методы автоматического обнаружения и сопровождения объектов // Обработка изображений и управление. – М.: Радиотехника. – 2008. – 176 с.
3. Анализ алгоритмов обнаружения и измерения координат объектов в оптико-электронных системах / О.В. Корзунов, А.И. Лужинский // Известия ТулГУ. Технические науки. 2017. Вып. 12. Ч. 3.
4. Варфоломеев А. Ю. Методи та алгоритми автоматичного відслідковування об'єктів на відеопослідовностях: монографія / А. Ю. Варфоломеев. – К.: КІМ, 2013.-112 с.

АНАЛІЗ ФУНКЦІОНАЛЬНОЇ ЖИВУЧОСТІ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ

¹Лисенко О.І., ³Самберг А., ²Чумаченко С.М., ¹Новіков В.І.

¹ *Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна*

² *Національний університет харчових технологій, Україна*

³ *Європейська організація з кібербезпеки, Бельгія*

E-mail: novikov1967@ukr.net, lysenko.a.i.1952@gmail.com,

ANALYSIS OF FUNCTIONAL VISIBILITY OF WIRELESS SENSOR NETWORKS

The report analyzes key components for formulating conceptual approaches to ensuring the functional viability of a wireless sensor network.

Структура аналізу живучості безпроводових сенсорних мереж (БСМ) полягає в дослідженні [1] критичних елементів БСМ, вихід з ладу яких призводить до розпаду мережі на незв'язані сукупності частини; зовнішніх та внутрішніх впливів, які призводять до загублення зв'язності; можливостей щодо відновлюваності раціональних показників функціонування мережі; кількісних показників, що характеризують живучість БСМ.

Загально-теоретично живучість забезпечується технологіями розпізнавання, протидії, відновлення, адаптації (інваріантності та квазіінваріантності), реконструкції, реконфігурації та реорганізації.

Технологія розпізнавання кібератаки у БСМ використовує методи: діагностики стану елементів мережі; ідентифікації взаємодіючих елементів; оповіщення центру управління мережею про наближення до критичного стану; реєстрації подій в мережі та умови їх виникнення; аналізу моделей поведінки елементів мережі.

Технологія протидії (технологія кризисного управління) БСМ спрямована на прогнозування моменту часу переходу БСМ на режим функціонування у нештатній ситуації і використовує методи: обґрунтування раціональної надмірності ресурсів у мережі; теорії ігрових рішень для мережі; авторизації елементів мережі.

Технології відновлення у БСМ використовують методи оперативного відновлення функціональної живучості для передбачуваних нештатних ситуацій (методи, які дозволяють заздалегідь розробити алгоритми за якими потрібно парировати нештатну ситуацію, яка точно ідентифікована як передбачувана).

Технології адаптації, інваріантності та квазіінваріантності у БСМ використовують методи оперативного відновлення функціональної живучості для непередбачуваних нештатних ситуацій (тобто методи, які дозволяють заздалегідь розробити алгоритми підтримання та відновлення функціональної живучості в умовах різних типів попередньої невизначеності).

Технології реорганізації, реконфігурації та реконструкції у БСМ використовують методи, які дозволяють відповідно розробити алгоритми оперативного перерозподілу функцій між елементами БСМ, перебудови структури обміну службовою та прикладною інформацією в БСМ та спланувати плавну нехтовно малу деградацію системи протягом максимального часу, коли цілі функціонування БСМ ще виконуються.

Техніко-технологічним прототипом концептуального підходу до побудови технології забезпечення функціональної живучості БСМ на основі використання мобільних телекомунікаційних платформ (МТАП) можливо вважати підхід, який використано в технології побудови Wireless Mesh Network (WMN). Mesh-мережі за своєю структурою складаються із декількох кластерів (в загальному випадку їх кількість не обмежена). В Mesh-мережі підтримується динамічна маршрутизація трафіку між точками доступу за оптимальним (за критерієм часу) маршрутом, забезпечується функціональна живучість мережі при відмовах деяких її елементів.

Стосовно БСМ можливо стверджувати, що базуючись на техніко-технологічному прототипі та комбінованому використанні наведених вище технологій є можливість розробляти конкретні методики, процедури та алгоритми забезпечення функціональної живучості безпроводової сенсорної мережі у вигляді методики формулювання кількісних показників живучості; процедури попереднього ретроспективного аналізу ситуацій втрати живучості; алгоритмів забезпечення зв'язності; алгоритмів забезпечення якості передачі сигналу; алгоритмів забезпечення пропускної здатності; алгоритмів управління взаємодією елементів БСМ.

Глобальна (регіональна) БСМ складається із деякої кількості мультисенсорних мобільних, квазімобільних та стаціонарних датчиків первинної інформації, тобто сенсорних вузлів. Підкреслимо, що сенсорні вузли (мобільні, квазімобільні і стаціонарні) можуть бути розташовані у різних середовищах: на дні водойм; під водою; на поверхні води; на твердій поверхні; у повітрі; у космічному просторі. Розглядається БСМ із сенсорними вузлами, що розташовані у різних середовищах. Вважається, що функціональна живучість БСМ забезпечена, якщо періодично через інтервал часу T_0 відбувається передача інформації, що зібрана із усіх сенсорів, які ще не відмовили, у центр управління. Під впливом внутрішніх та зовнішніх збурень мережа втрачає свою цілісність, тобто розпадається на деяку кількість сукупностей сенсорних вузлів, які зберігають зв'язність лише в цій сукупності (кластері). Підкреслимо, що щільність розташування сенсорних вузлів та запас енергетичного ресурсу кожного сенсорного вузла буде різною. Необхідно підтримати спроможність, вже не цілісної мережі, а набору сенсорних сукупностей, передати усю накопичену при кінці кожного інтервалу часу T_0 до центру управління. На відміну від БСМ неперервного часу (або як кажуть оперативних систем чи систем реального часу) в БСМ дискретного часу (або як кажуть Delay Tolerant Networks) можливо використати мобільні платформи (підводні, надводні, повітряні або навіть космічні, зрозуміло, в залежності від середовища розташування сенсорних

вузлів БСМ) для збирання інформації та (або) відновлення зв'язності мережі і підвищення її пропускної здатності із заданою якістю передавання інформації. Ключовими складовими для формулювання концептуальних підходів до забезпечення функціональної живучості безпроводової сенсорної мережі на основі використання МТАП є [2]:

1. Ідентифікація та прогнозування на один чи декілька періодів спостереження вектору стану кожного елемента БСМ (сенсорних вузлів, маршрутизаторів, шлюзів контролерів): просторових координат; залишку енергії в акумуляторній батареї; результати самоконтролю внутрішніх параметрів елементів БСМ; об'єм та важливість даних моніторингу, які очікують на передавання у наступному циклі.

2. Призначення головного вузла (вузла, який займається збором інформації із закріплених за ним на поточний цикл сенсорних вузлів).

3. Розрахунок траєкторії руху МТАП для зчитування інформації з головного вузла.

Концептуальний підхід до забезпечення функціональної живучості безпроводової сенсорної мережі на основі використання МТАП передбачає, що в якості вихідних даних повинні бути відомі: початкова просторова структура та якісний і кількісний склад БСМ (тобто із яких елементів складається БСМ та їх технічні характеристики, включаючи і показники мобільності); алгоритм самоорганізації, визначення просторових координат, управління радіотехнічними та телекомунікаційними параметрами елементів БСМ; технічні характеристики МТАП (як ті, що складають вектор телекомунікаційних параметрів, так і ті, що складають вектор, що описує динаміку руху платформи).

Припускаємо, що безпроводовий обмін інформацією із зануреними під воду елементами БСМ реалізується завдяки акустичним сигналам, а у повітряному та космічному просторі використовуються радіотехнічні та лазерні технології передачі та приймання телекомунікаційних сигналів.

Для прийняття рішення щодо забезпечення функціональної живучості БСМ необхідно сформулювати критерій цієї функціональної живучості. Зважаючи на те, що БСМ є елементом інформаційно-керуючої системи, в якій для прийняття управлінських рішень потрібно отримувати інформацію від БСМ із періодом не більше T_0 , пропонується прийняти критерій функціональної живучості БСМ у вигляді: реальний час, який витрачається на збір інформації у БСМ не перевищує T_0 .

Література

1. Марченко В.С., Яковлев С.В., Горбатчик О.С. та ін. Забезпечення функціональної безпеки критичних інформаційно-керуючих систем: монографія / за ред. В.С. Марченка, С.В. Яковлева. Харків: Константа, 2019. 272 с. ISBN 978-966-342-415-6.
2. Romaniuk V. Increasing the efficiency of data gathering in clustered wireless sensor networks using UAV / V. Romaniuk, O. Lysenko, A. Romaniuk and O. Zhuk // Information and telecommunication sciences. – 2020. - Vol. 11, no. 1. - С. 102-107. – DOI: <https://doi.org/10.20535/2411-2976.12020.102-107>.

ЗАСТОСУВАННЯ МУЛЬТИМЕТРИЧНИХ ПРОТОКОЛІВ ТА МІЖШАРОВОГО ПІДХОДУ ДЛЯ ПІДВИЩЕННЯ ЕНЕРГОЕФЕКТИВНОГО ФУНКЦІОНУВАННЯ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ

Новіков В.І.¹, Дворська С.В.^{1, 2}, Дакова Л.В.²

¹ *Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна*

² *Державний університет телекомунікацій, Україна*

E-mail: novikov1967@ukr.net, dvorskaya80@ukr.net, dacova@ukr.net

STAGNATION OF MULTIMETRIC PROTOCOLS AND MULTI-BALL APPROACH FOR THE ADVANCEMENT OF ENERGY-EFFICIENT FUNCTION OF WIRELESS SENSOR FENCES

In addition, there are presented business procedures for reaching compromises between business goals in wireless sensor networks, including energy savings. An algorithm has been propagated that will allow you to unify the re-routing of the system.

Мультиметричні (багатометричні) протоколи використовують різні мережеві вимірювання для задоволення кількох потреб у застосуванні. Наприклад, протоколи маршрутизації, що стосуються конкретних програм, пропонують поєднувати енергоефективність із вимогами QoS [1–2]. Ці дослідницькі роботи враховують запаси енергії вузлів разом із спотворенням даних, швидкістю помилок пакетів або стану вузла. Однак такий різновидовий протокол викликає нові проблеми. Зазвичай протоколи маршрутизації покладаються на вагову функцію різних показників, а коригування даних часто проводиться за методологією проб і помилок. Більше того, мультиметричні протоколи маршрутизації вимагають визначення вичерпних показників та їх підтримку у кожному вузлі, що створює додатковий обмін повідомленнями. Наприклад, якість посилення може бути оцінена лише статично за допомогою індикатору рівня отриманого сигналу RSSI (Received Signal Strength Indicator), індикатора якості радіоканалу LQI (Link Quality Indicator) або показника швидкості прийому пакетів, який змінюється з часом. Таким чином, ці протоколи мають недоліки у вигляді додаткових накладних витрат, але з іншого боку, вони дозволяють вдосконалити адаптацію до змін стану мережі, оскільки рішення вузлів базуються на показниках, зміна яких відображає стан мережі. Нижче представлено аналіз деяких багатометричних протоколів з точки зору їх енергоефективності:

1). Маршрутизація за допомогою протоколу ATSR, де рішення про маршрутизацію приймаються локально на основі вагової функції, яка враховує залишкову енергію сусідніх вузлів, їх розташування та довіру. Для оцінки рівня зношення сусіднього датчика використовується такі показники безпеки, як стан вузла, автентифікація та цілісність повідомлення для

виявлення шкідливих вузлів. Протокол вимагає додаткових керуючих повідомлень для оцінки енергії сусідніх вузлів, а рівень довіри та ваги повинні бути відрегульовані для обміну безпекою та енергією.

2) ERTLD – протокол удосконаленої маршрутизації в режимі реального часу з розподілом навантаження на вузли, де оптимальні рішення щодо переадресації приймаються на основі RSSI. Протокол ERTLD може доставляти пакети в терміни від кінця до кінця, підвищуючи гнучкість, оскільки це може уникнути проблеми маршрутизації пустих місць. Більше того, він має більш високий коефіцієнт доставки і споживає менше енергії, ніж сучасні рішення.

3) REMuR – це ієрархічний протокол маршрутизації пакетів через стаціонарну WSN, задовольняючий як енергоефективність, так і вимоги QoS. У цьому рішенні головний вузол СН (Cluster Head) вибирає шлях до базової станції BS (Base Station), рівень енергії якої, що залишилася після передачі, буде найвищою серед усіх можливих шляхів. Якщо доступної пропускної здатності недостатньо, СН може вирішити скинути менш значні пакети відповідно до їх впливу на загальне псування даних. Протокол REMuR добре підходить для програм спостереження, контролю руху та моніторингу стану здоров'я. Однак формування кластерів є централізованою процедурою, тому воно створює додаткові накладні витрати: кожен вузол надсилає інформацію про свою енергію та місце розташування до BS.

4) Алгоритм InRout вирішує вибір маршруту для промислових безпроводових сенсорних мереж, щоб забезпечити високу надійність, враховуючи обмежені ресурси сенсорних вузлів. Рішення використовує Q-навчання для вибору найкращого можливого маршруту, виходячи з поточних мережеских умов та налаштувань програми. Вузол вибере маршрут, який максимізує його успіх щодо коефіцієнта помилок пакетів (PER) та енергії вузла.

У випадку використання міжшарового підходу було проведено багато досліджень для вирішення споживання енергії на всіх шарах, особливо в мережі MAC та фізичних шарах. Очікується, що інтегрована міжшарова конструкція може значно підвищити енергоефективність, а також адаптованість до динамічних середовищ. Дійсно, міжшарові рішення використовують взаємодію між різними шарами для оптимізації роботи мережі. Вимоги до датчиків (QoS, маршрутизація, термін експлуатації, безпека тощо) тісно пов'язані між собою і потребують всебічного вивчення існуючих компромісів. Різностарові рішення дозволяють вирішити взаємозалежність цих проблем. В якості конкретного прикладу можна відстежувати рівень стану акумулятора на фізичному рівні і використовувати цю інформацію на рівні MAC для справедливого призначення слотів зв'язку для вузлів. Аналогічно можна розглянути графік завад при маршрутизації даних для оптимізації передачі затримки. Зміни топології, ймовірно, відбудуться у WSN та можуть скористатися підходом міжшарового рівня.

Наприклад, після додавання чи видалення вузла змінюється щільність мережі та кількість перешкод на фізичному рівні. Таким чином, може

знадобитися перерозподіл слотів або відповідна зміна на рівні MAC, створюючи різні можливості для вибору шляху на сегменті маршрутизації. В роботі [3] автори в спільній маршрутизації протоколів MAC та фізичному рівні, для розподілу енергії в кооперативних мережах датчиків зв'язку під заданою швидкістю пакетної помилки (PER) пропонують енергоефективний алгоритм вибору координатора PAN у сенсорних мережах на базі IEEE 802.15.4 Вони поєднують процедуру формування мережі, визначену на рівні MAC, з алгоритмом реконфігурації топології, що працює на мережевому рівні. За рахунок мінімізації висоти їхнього кластеру алгоритм може зменшити затримку і продовжити термін служби мережі.

В роботі [4] автори пропонують вигляд мережі між сегментами маршрутизації та MAC. Їх протокол маршрутизації на основі кластерів врівноважує навантаження між вузлами, будуючи кілька шляхів, заснованих на силі сигналу та кількості стрибків. У протоколі MAC на основі TDMA голова кластера адаптивно призначає слоти активним вузлам на основі типу трафіку. Їх рішення зменшує споживання енергії та затримку, і досягає високих коефіцієнтів пропускної здатності та доставки пакетів, вибираючи шляхи з кращою якістю зв'язку та уникаючи зіткнень та перешкод.

Запропоновано алгоритм, коли вузол датчика знає власне географічне розташування, використовуючи GPS, а також знає про всі місця своїх сусідніх датчиків. Крім того, кожен вузол знає місцеположення низхідного вузла. Удосконалена версія цього алгоритму пропонується у посиленнях, який використовує ємність буфера і порівнює буфер вузлів, що в свою чергу сприятиме уникненню перенавантажень. У інших дослідженнях для того, щоб використовувати багатосмугову маршрутизацію, тобто балансування навантаження, пропонується збільшити пропускну здатність мережі. Більше того, запропонований алгоритм є гібридним, тобто таким, який виконує уникнення перевантажень із використанням удосконаленої маршрутизації. Він також нормалізує довжину черги та глибину кінцевого вузла від сенсорних вузлів. Іншими словами, він підтримує таблицю маршрутизації для найменшої глибини або найкоротшого маршруту.

Література

1. S. Sudevalayam, P. Kulkarni, Energy Harvesting Sensor Nodes: Survey and Implications, IEEE Communications Surveys & Tutorials 13 (2011) 443–461 с.
2. A. Prayati, C. Antonopoulos, T. Stoyanova, C. Koulamas, G. Papadopoulos, A modeling approach on the TelosB WSN platform power consumption, Journal of Systems and Software 83 (2010), 202–207 с.
3. J. Ko, C. Lu, M. B. Srivastava, J. A. Stankovic, A. Terzis, M. Welsh, Wireless Sensor Networks for Healthcare, Proceedings of the IEEE 98 (2010) 1947–1960 с.
4. A. Hadjidj, M. Souil, A. Bouabdallah, Y. Challal, H. Owen, Wireless Sensor Networks for Rehabilitation Application: Challenges and Opportunities, J. of Network and Computer Applications 36 (2013) 1–15 с.

АНАЛІЗ ВПЛИВУ КОНФІГУРАЦІЇ СЕНСОРНОЇ МЕРЕЖІ НА ТОЧНІСТЬ ВИЗНАЧЕННЯ МІСЦЕПОЛОЖЕННЯ ДЖЕРЕЛА РАДІОВИПРОМІНЮВАННЯ НА ОСНОВІ АОО-ВИМІРЮВАНЬ

Товкач І.О., Васильєв В.М., Чмельов В.О., Путієнко О.М.

*Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"*

ANALYSIS OF THE INFLUENCE THE SENSOR NETWORK CONFIGURATION ON THE ACCURACY OF DETERMINING THE RADIO SOURCE LOCATION BASED ON AOA MEASUREMENTS

The analysis of the number of sensor pairs of the sensor network on the accuracy of determining the location of the radio source based on AOA measurements using an isoline family is carried out. The analysis was performed using statistical modeling.

Однією з основних характеристик систем пасивної локації є сімейство ізоліній середнього квадратичного відхилення (СКВ) помилки вимірювання дальності джерела радіовипромінювання (ДРВ) побудованих в координатах x, y [1,2]. Кожна ізолінія, починаючи від центру, обмежує область, де помилка не перевищує 10 м, 20 м, 30 м, 40 м, відповідно. Задаючи, таким чином, допустиме значення СКВ $\sigma_{r_{don}}$ можна визначити область відстаней, в якій значення СКВ буде дорівнювати $\sigma_r \leq \sigma_{r_{don}}$. За швидкістю зміни відстаней між ізолініями можна також виявити азимутальні напрямки, де помилки в міру віддалення від центру ростуть повільніше або швидше.

Графіки сімейства ізоліній для випадку СКВ помилки вимірювання кута $\sigma = 0.8^\circ$, побудовані для трьох конфігурацій сенсорної мережі з різним числом пар датчиків сенсорної мережі, розташованих на колі радіусом 100 м.

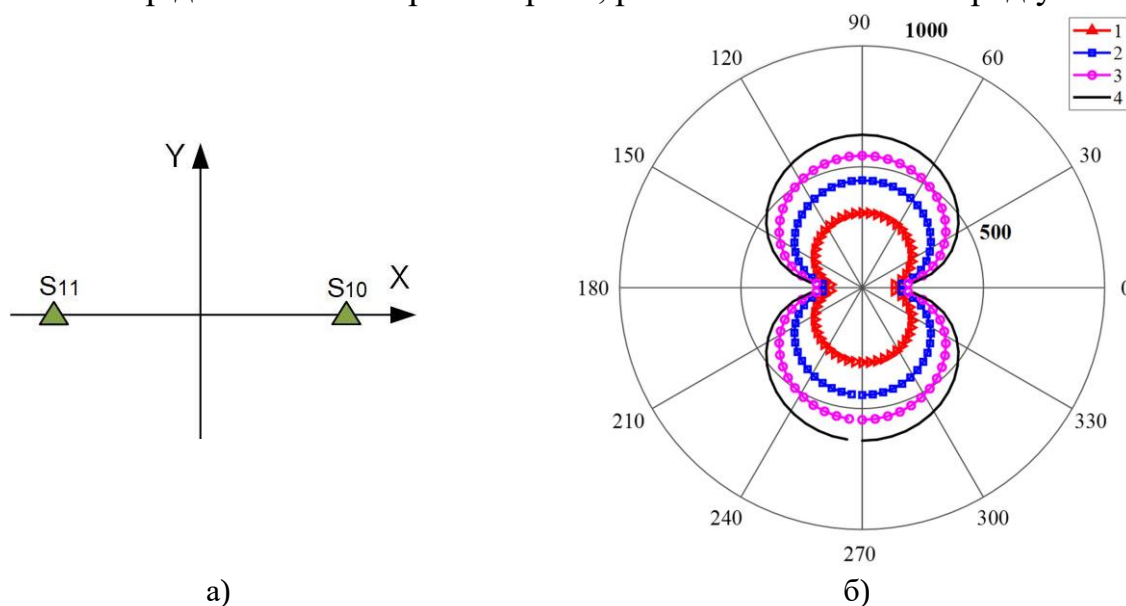


Рис. 1. Перша конфігурація сенсорної мережі.

Перша конфігурація сенсорної мережі складається з однієї пари датчиків рис. 1(а). При АОА-вимірюваннях рис. 1(б), СКВ помилки визначення місцеположення, в залежності від напрямку, носить нерівномірний характер. В напрямках 90° , 270° , воно росте найбільш повільно і не перевищує допустимого значення $\sigma_r \leq 10, 20, 30, 40$ м на відстанях 309, 444, 546, 632 м, відповідно. При невеликих кутах між базою і напрямком на ДРВ, на азимутах 0° , 180° , СКВ помилки визначення місцеположення є великим і не входить в діапазон допустимих значень.

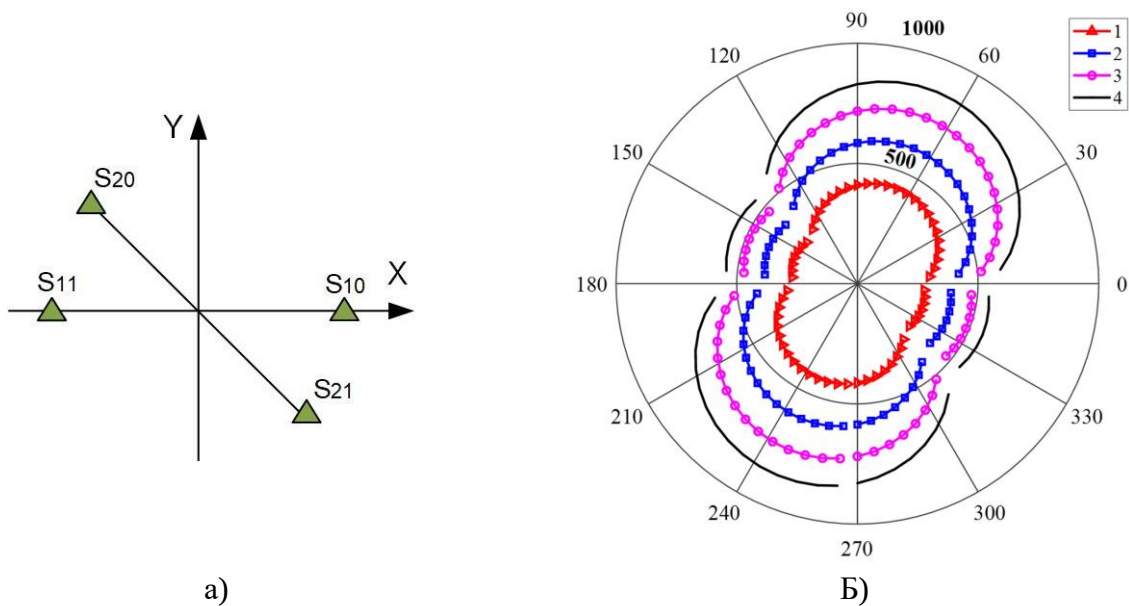


Рис. 2. Друга конфігурація сенсорної мережі.

Друга конфігурація сенсорної мережі складається з двох пар датчиків рис. 2(а). При АОА-вимірюваннях рис. 2(б), СКВ помилки на азимутах $67,5^\circ$, $247,5^\circ$ ростуть рівномірно і не перевищують допустимих значень $\sigma_r \leq 10, 20, 30, 40$ м на відстанях 427, 607, 744, 860 м, відповідно. При невеликих кутах між базою і напрямком на ДРВ, на азимутах 0° , 135° , 180° , 315° , СКВ помилки визначення місцеположення є великим і не входить в діапазон допустимих значень.

Третя конфігурація сенсорної мережі складається з чотирьох пар датчиків рис. 3(а) [3]. При АОА-вимірюваннях рис. 3(б), СКВ помилки на азимутах 0° - 360° ростуть рівномірно і не перевищують допустимих значень $\sigma_r \leq 10, 20, 30, 40$ м на відстанях 513, 710, 871, 1000 м, відповідно. При невеликих кутах між базою і напрямком на ДРВ, на азимутах 0° , 45° , 90° , 135° , 180° , 225° , 270° , 315° , СКВ помилки визначення місцеположення є великим і не входить в діапазон допустимих значень.

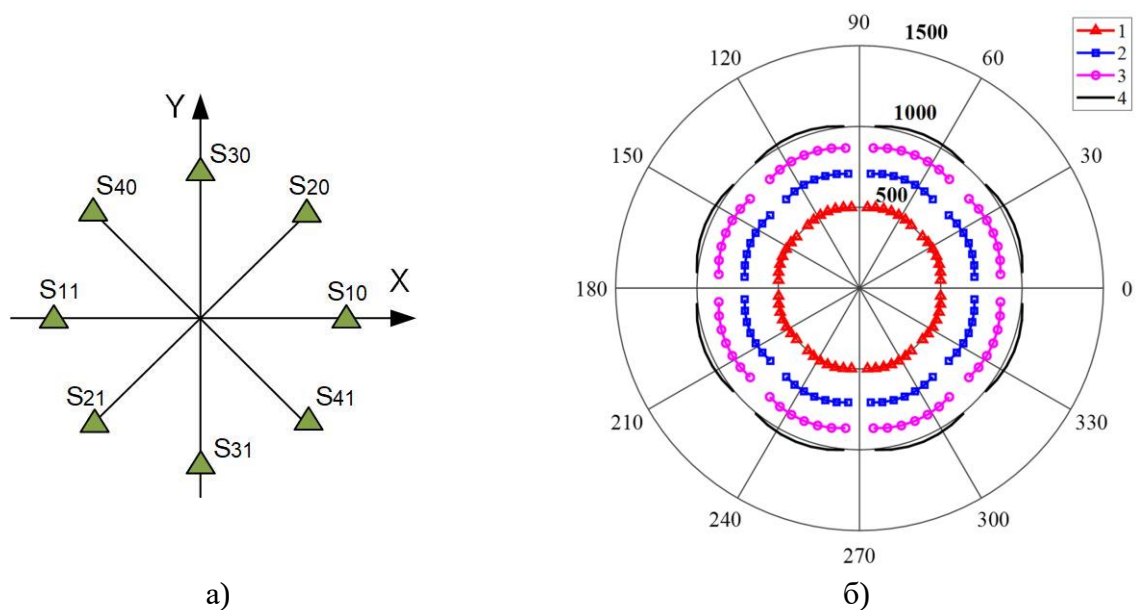


Рис. 3. Третя конфігурація сенсорної мережі.

При збільшенні числа пар датчиків сенсорної мережі, ізолінії зберігають форму концентричних кіл і при цьому істотного приросту в точності визначення місця розташування ДРВ не відбувається. Тому, розглянута топологія мережі з чотирьох пар датчиків, може бути рекомендована для використання на практиці, якщо напрямок появи цілі невідомо.

Висновки. Конфігурація з чотирьох пар датчиків сенсорної мережі, які розташовані рівномірно по колу, забезпечують вид ізоліній, що обмежують область в яких кругове СКВ не перевищує задане значення, також у вигляді кіл в горизонтальній площині. При подальшому збільшенні числа датчиків сенсорної мережі, істотного приросту в точності визначення місцеположення ДРВ не відбувається, і вона може бути рекомендована, якщо напрямок появи цілі невідомий.

Література

1. I. O. Tovkach, S. Y. Zhuk, O. S. Neuimin and V. O. Chmelov, "Recurrent Algorithm Of Passive Location In Sensor Network By Angle Of Arrival Of A Signal," 2020 IEEE 40th International Conference on Electronics and Nanotechnology (ELNANO), Kyiv, Ukraine, 2020, pp. 728-732, doi: 10.1109/ELNANO50318.2020.9088740.
2. Симаков В.А. Построение адаптивных систем пассивной радиолокации на принципах разностно-дальномерной координатометрии / В.А. Симаков // Научные ведомости Белгородский государственный университет . — 2005. — №2. — С. 221.
3. Товкач И.О. Фильтрация параметров движения источника радиоизлучения на основе угломерных измерений сенсорной сети / И.О. Товкач, С.Я Жук // XIV Міжнародна Науково-технічна Конференція "Перспективи телекомунікацій 2020", 13.04-17.04.2020р.: тези доп. — Київ, 2020. <http://conferenc.its.kpi.ua/2020/paper/view/20283>.

АНАЛІЗ ТЕХНОЛОГІЙ ТА ПАРАМЕТРІВ ФУНКЦІОНУВАННЯ ІОТ МЕРЕЖ

Лапа Є.О., Лисенко О.І., Савченко А.О.

*Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: lapa.yegor@gmail.com*

ANALYSIS OF TECHNOLOGIES AND OPERATING PARAMETERS OF IOT NETWORKS

This article describes and compares three main IoT communication technologies: Bluetooth Low Energy, 6LowPAN and ZigBee, using the following operating parameters – distance range, network throughput, and packet delay. All technologies have its own advantages and disadvantages, but as «golden mean» we can consider 6LowPAN.

Для побудови мережі інтернету речей (IoT) на сьогодні розробляються досить багато різних технологій, серед яких відомі такі як: IEEE 802.11 (WiFi), IEEE 802.15.4 (ZigBee), Bluetooth Low Energy (BLE), 6LowPAN (Thread), LoRaWAN, Z-wave, SIGFOX, NFC та інші [1]. Однак в літературі недостатньо приділено уваги практичному порівнянню даних технологій, що ускладнює вибір раціонального рішення для тої чи іншої задачі. Тому метою даної роботи є порівняльний аналіз основних особливостей та характеристик таких технологій як BLE, 6LowPAN (Thread) і LoRaWAN та розробка рекомендації щодо їх застосування.

Однією із найрозповсюдженіших технологій, яка тісно пов'язана з нашим життям стала BLE (Bluetooth Low Energy). Енергоефективність BLE зробила його кращим та одним із найбільш сумісних варіантів IoT. Наприклад, BLE є більш енергоефективним, ніж ZigBee, Bluetooth classic та Wi-Fi. Це означає, що BLE може краще підтримувати підключення пристроїв IoT протягом довших періодів, ніж зазначені вище (особливо, коли пристрої працюють від батареї). Крім того, низька швидкість передачі даних BLE робить її надзвичайно придатною для використання в тих випадках, коли потрібно обмінюватися лише даними стану, наприклад датчиками. У наш час це також домінуюча технологія низького енергоспоживання у смартфонах, на відміну від ZigBee, Z-Wave, LoRa та інших [2].

Ще однією технологією, яка щільно пов'язана з нашим життям є 6LowPAN. 6LowPAN – відкритий стандарт, визначений в RFC 6282 Робочою групою інженерів Інтернету (IETF). Особливість 6LowPAN полягає в тому, що він був спочатку задуманий, щоб підтримувати малопотужні бездротові мережі 2,4 ГГц, побудовані на базі IEEE 802.15.4, але тепер цей стандарт адаптований і використовується в безлічі інших середовищ мережевий передачі, включаючи бездротові мережі в діапазонах нижче 1 ГГц, Smart Bluetooth, передачу даних по лініях електропередачі (PLC) і малопотужні мережі Wi-F [3].

Одним з перших гравців в технологіях протоколів IoT є ZigBee. Основними ідеями цієї технології є швидкість передачі даних може

становити від 20 до 250 кбіт/сек, Дальність дії – до 100 м. Завдяки низькому рівню енергоспоживання мережі ZigBee можуть працювати по кілька років від однієї батареї. Особливістю ZigBee є можливість підтримки комірчастої топології, що дозволяє мережі самовідновлюватися і продовжувати передачу пакетів даних при обриві зв'язку між вузлами.

Порівнюємо характеристики технологій за різними показниками, скориставшись дослідженнями Ericsson и Silabs. В таблиці 1 наведено порівняння характеристик дальності роботи при різній вихідній потужності.

Таблиця 1. Порівняння дальності роботи протоколів IoT.

Вихідна потужність [дБм]	0	+4	+8
Bluetooth Low Energy	248	276	345
6LowPAN	209	270	328
ZigBee	196	231	280

Виходячи з даних таблиці, можна зробити висновок, що найбільшу дальність дає Bluetooth Low Energy, на другому місці йде 6LowPAN, яка гірша на 2-5%, а в кінці технологія ZigBee з показниками гірше на 16-18%.

Розглянемо пропускну здатність в залежності від кількості стрибків (рис.1).

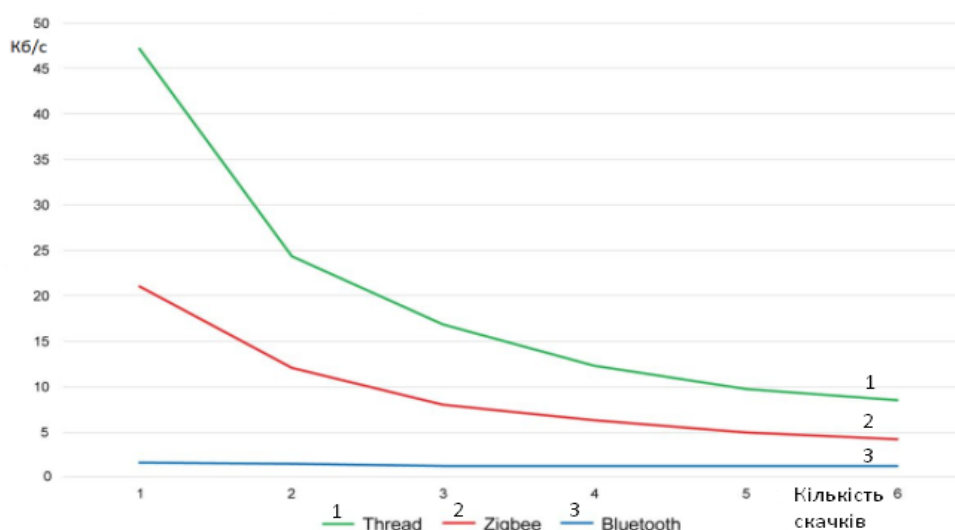


Рис.1. Пропускна здатність в залежності від кількості скачків (hop).

Виходячи з графіка, можна зробити висновок, що 6LowPAN показує швидкість 46 кбіт/с, а це 75% від символної швидкості радіопередавача (62,5 кбіт/с). Це означає, що висока ефективність протоколів маршрутизації. Порівнявши ZigBee з 6LowPAN можна зробити висновок, що перша в свою чергу поступається приблизно у 2 рази при рівних умовах. Bluetooth Low Energy майже не залежить від кількості вузлів і складає приблизно 2-3 кбіт/с.

Також порівняємо затримку в залежності від розмірів пакетів даних (рис.2).

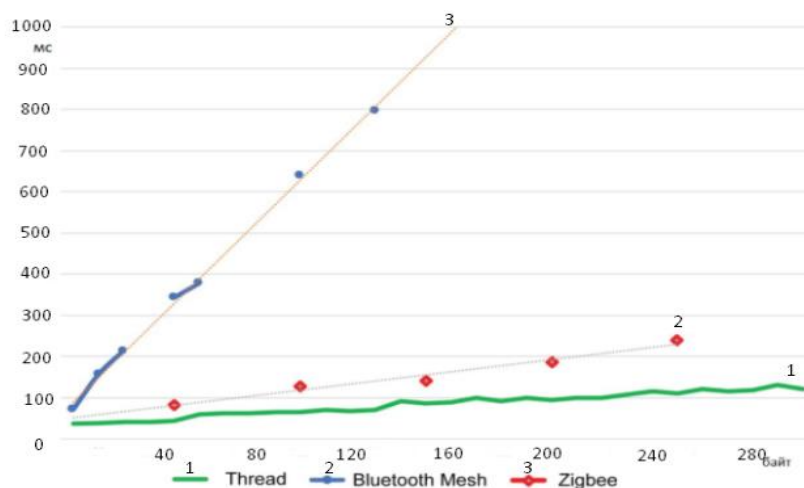


Рис.2. Затримка в залежності від розмірів пакетів даних.

Із графіка видно, що при невеликій кількості передачі даних всі протоколи забезпечують приблизно однаковий результат. Всі мережі забезпечують лінійну залежність затримок залежно від розмірів передачі даних. Найкраще себе показала технологія 6LowPAN. ZigBee показує гарну ефективність, але і велику фрагментацію на рівні додатків. Затримки в Bluetooth Low Energy виростають із збільшенням передачі даних. Це виникає із-за малих розмірів пакетів та сегментації [4].

Отже, можемо зробити наступний висновок, що на сьогоднішній день існує досить багато технологій, які роблять IoT все більш доступним. Одні з них вже працюють не один рік, інші лише розпочинають свій шлях, тому кожна з них має свої переваги, але в свою чергу і недоліки. Порівнявши параметри 6LowPAN, ZigBee та Bluetooth Low Energy, не можна однозначно вирішити який протокол використовувати сьогодні для IoT мережі. На нашу думку 6LowPAN є яскравим представником тієї технології, яка скрізь має «золоту середину». У неї не найкраща дальність роботи, але близька до лідера, пропускна здатність висока, отже і ефективність також, а затримка нижча в порівнянні з її конкурентами.

Література

1. Wireless Protocols for Internet of Things [Електронний ресурс]. – Режим доступу: <https://medium.com/blueeast/wireless-protocols-for-internet-of-things-7ed0bd860c66>.
2. Д. Денисов, К. Брагін “Введення в концепцію "інтернету речей" (IoT)” [Електронний ресурс]. – Режим доступу : <https://nag.ru/articles/article/107810/vvedenie-v-kontseptsuyu-interneta-veschey-iot.html> – Дата публікації: 30.09.2020.
3. Mohammad Afaneh “Bluetooth Low Energy (BLE) and the Internet of Things (IoT)” [Електронний ресурс]. – Режим доступу : <https://www.linkedin.com/pulse/bluetooth-low-energy-ble-internet-things-iot-mohammad-afaneh/> – Дата публікації: 26.04.2017.
4. Практическое сравнение ячеистых сетей (thread, zigbee, ble mesh) [Електронний ресурс]. – Режим доступу: <https://r-iot.org/2019/05/12/практическое-сравнение-ячеистых-сет/> – Дата публікації: 12.05.2019.

РОЗВИТОК МЕТОДІВ МАРШРУТИЗАЦІЇ В МОБІЛЬНИХ СЕНСОРНИХ МЕРЕЖАХ

Штойко О.О., Лисенко О. І.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: shtoyko1999@gmail.com

DEVELOPMENT OF ROUTING METHODS IN MOBILE SENSOR NETWORKS

The article describes an example of the implementation of a mobile sensor network based on the protocol RASeR and its advantages.

Метою роботи є порівняльний аналіз протоколу маршрутизації RASeR (Robust Ad-hoc Sensor Routing) з такими відомими протоколами, як MACRO (MAC / Routing protocol), OLSR (Optimized Link-State Routing) і AODV (Ad hoc OnDemand Distance Vector), відносно бездротової сенсорної мережі з мобільними вузлами. Передбачається, що даний протокол буде використовуватися в бездротової сенсорної мережі для забезпечення зв'язку групи безпілотних літальних апаратів.

RASeR використовує техніку сліпого пересилання в БСМ для передачі пакетів приймача, а також протоколи управління доступом до середовища (MAC рівень) з тимчасовим поділом каналів (TDMA) для вирішення проблеми підтримки актуального градієнта в топології, що змінюється без ризику виникнення широкомовного шторму. Таким чином, кожен вузол здійснює розсилку в певному порядку, відповідно за часовим інтервалом - слотом, тривалість якого розрахована для передачі одного пакета. Тривалість тимчасових інтервалів і номери вузлів встановлюються до розгортання мережі, що робить протокол RASeR адаптованим. Оскільки кожен вузол знає, коли очікується запуск кожного слоту під час прослуховування широкомовної передачі іншого вузла, він порівнює час прибуття пакета з початком відліку очікуваного запуску. Крім того, якщо для отримання інформації про місцезнаходження використовується система навігації, то кожен вузол може синхронізувати свій годинник з отриманим часом із супутників.

Протокол RASeR використовує метод сліпого пересилання, при цьому рішення про пересилання даних проводиться приймальним вузлом на основі значення кількості переходів до приймального вузла. Таким чином, коли вузол виконує розсилку, пакет приймається всіма сусідами в зоні видимості. Потім кожен сусідній вузол порівнює кількість переходів, яке відоме з прийнятого пакета, зі своїм власним. Потім, якщо кількість переходів вузла менша, ніж кількість переходів в прийнятому пакеті, пакет повинен бути переадресований. Якщо власне кількість переходів вузла більше, ніж кількість переходів в прийнятому пакеті, пакет видаляється, а якщо ці величини рівні, необхідно враховувати пріоритет пакетів. Пріоритети

використовуються для управління кількістю маршрутів, тим самим надлишкове дублювання пакетів в мережі зводиться до мінімуму і в той же час підвищується надійність протоколу через різноманітність маршрутів. Загальний алгоритм роботи в кожному часовому інтервалі для вузлів мережі, побудованої на основі протоколу маршрутизації RASeR, показаний на рис. 1 у вигляді блок-схеми.

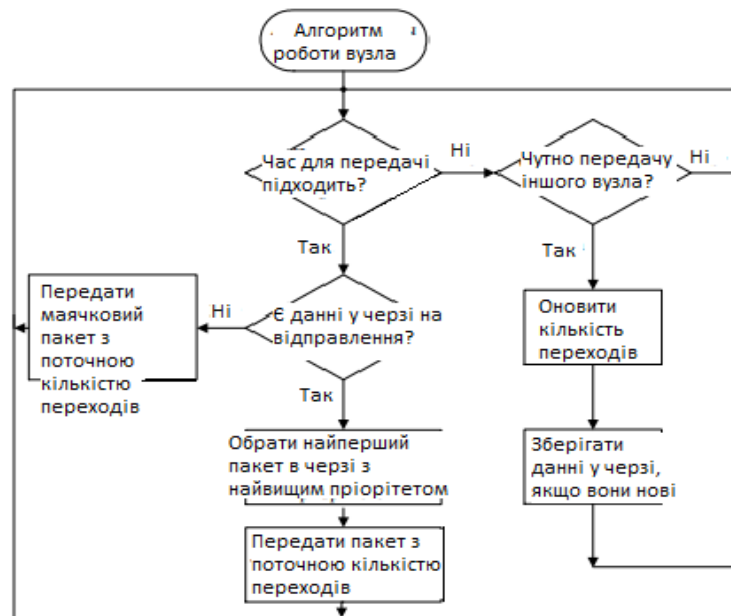


Рис. 1. Алгоритм роботи вузла протоколу RASeR.

Ключовими характеристиками протоколу RASeR, які роблять його надійним, є те, що кожен вузол може виступати маршрутизатором, що здійснює розгалуження маршруту передачі пакету. З цього випливає, що можлива реалізація одночасно декількох напрямків до базової станції, що значно знижує втрату пакетів при частих змінах топології мережі. Крім того, оскільки кожен вузол поводить себе однаково, це дозволяє підтримувати протокол простим і може дозволити організувати мережу з великою кількістю вузлів. Для оцінки продуктивності протоколу RASeR далі представлені порівняльні характеристики з іншими протоколами відповідно до заданих критеріїв при різних швидкостях пересування вузлів, масштабованості, а також при різних навантаженнях трафіку мережі. Характеристики протоколу маршрутизації RASeR отримані в результаті моделювання в програмному середовищі MATLAB [1].

Вихідні дані, які використовувалися при моделюванні, представлено в таблиці 1. Дані протоколів AODV, OLSR, MACRO були отримані в [2] шляхом моделювання в програмному середовищі OPNET Modeler [3].

Результати порівняльних характеристик протоколів (див. таблиці 2) продемонстрували, що протокол RASeR має перевагу над іншими в разі зміни швидкості пересування вузлів мережі. Однак рівень середнього споживання енергії даного протоколу незначно поступається протоколу MACRO.

Таблиця 1. Вихідні данні для моделювання.

Кількість вузлів в мережі	n	25
Довжина однієї сторони квадратної області мережі, м	L	600
Радіус покриття вузлів, м	r	200
Швидкість передачі, біт, кбіт/с	R_b	250
Максимальна швидкість переміщення вузлів, м/с	V_{max}	25
Швидкість генерації пакету, пакет/с	f_p	1
Розмір даних, що генеруються, біт	L_{data}	32
Загальний розмір пакету, біт	L_p	47
Напруга живлення, В	V_{batt}	3
Струм при передачі даних, мА	I_{tx}	16,5
Струм при прийомі даних, мА	I_{rx}	15,5

Таблиця 2. Результати порівняльних характеристик протоколів.

	Швидкість пересування вузлів, м/с	MACRO	OLSR	AODV	RASeR
Коефіцієнт доставки пакетів (PDR)	3	1	0,46	0,74	1
	10	0,99	0,5	0,77	0,99
	20	0,98	0,51	0,74	0,98
	40	0,97	0,53	0,73	0,98
Середня наскрізна затримка	3	0,05	0,138	1,2	0,01
	10	0,065	0,131	1,18	0,01
	20	0,075	0,125	1,21	0,01
	40	0,06	0,121	1,23	0,01
Середні непродуктивні витрати, біт	3	112	480	640	77
	10	119	460	505	77,6
	20	120	464	479	77,8
	40	123	465	466	78
Пропускна здатність, біт/с	3	641	300	499	718
	10	640	349	511	718,4
	20	639	358	510	718,2
	40	639	359	506	717
Середнє споживання енергії, Дж/с	3	0,0017	0,0146	0,0163	0,0036
	10	0,0018	0,0149	0,0174	0,0036
	20	0,0019	0,0142	0,0178	0,0037
	40	0,0021	0,0141	0,0176	0,0037

Використання протоколу RASeR циклічного характеру управлінням доступу до середовища виключає появу широкомовного шторму, а також, незважаючи на відсутність механізму запобігання зіткнень і повторних передач, зберігає надійність доставки пакетів навіть при високій частоті зміни топології. У разі виходу з ладу будь-якого з вузлів мережі, існує можливість його заміни працездатним вузлом з таким же ідентифікаційним номером, що не вплине на якість обслуговування мережі.

Література

1. MATLAB Analyze data, develop algorithms, and create mathematical model [Електронний ресурс. – Режим доступу: <https://www.mathworks.com/>].
2. Hayes T., Ali F.H. Robust Ad-hoc Sensor Routing (RASeR) protocol for mobile wireless sensor networks // Ad Hoc Networks. – 2016. – P. 128–144.
3. OPNET is now part of Riverbed [Електронний ресурс. – Режим доступу: <https://www.riverbed.com/gb/products/steelcentral/opnet.html?redirect=opnet?redirect=opnet>

РОЗВИТОК АЛГОРИТМІВ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ MIMO У МОБІЛЬНИХ СЕНСОРНИХ МЕРЕЖАХ

Сергійчук Д. М., Лисенко О. І.

Інститут телекомунікаційних систем КІІ ім. Ігоря Сікорського, Україна

E-mail: s99danil@gmail.com

DEVELOPMENT OF ALGORITHMS FOR APPLYING MIMO TECHNOLOGY IN MOBILE SENSORY NETWORKS

The report discusses: Wireless sensor networks. Increase bandwidth. MIMO technology. Advantages and advantages of MIMO. Application of MIMO technology in IEEE 802.11ac. MIMO in Wireless Touch Networks.

Безпроводова сенсорна мережа (БСС) виникає тоді, коли велику кількість датчиків інформаційно об'єднують для спільного контролювання значного фізичного середовища. Мобільна БСС – це різновид БСС. Сенсорні вузли спілкуються не тільки один з одним, але і з базовою станцією (БС), через бездротові канали, що дозволяє їм надавати зібрані дані для віддаленої обробки, візуалізації, аналізу та зберігання. Наприклад, на рисунку 1 показано дві групи датчиків, які контролюють два різних географічних регіонів і підключення до Інтернету за допомогою базових станцій.

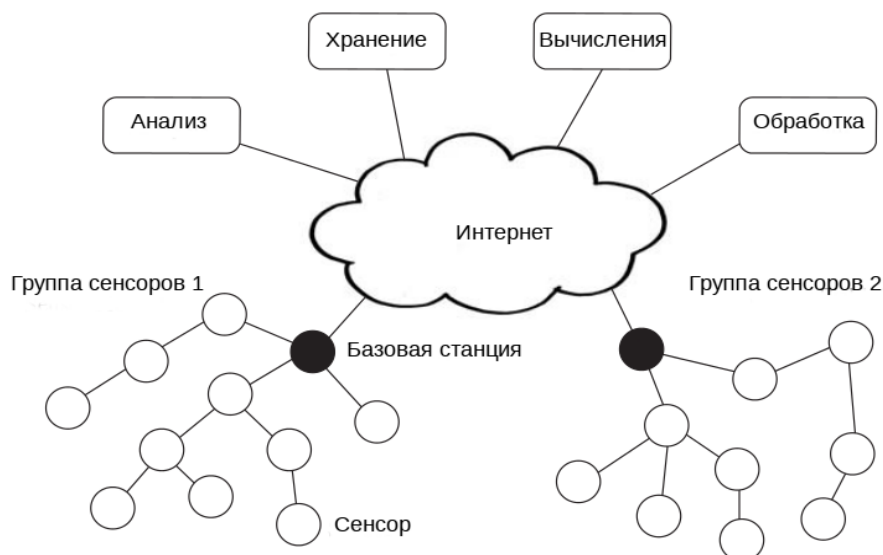


Рис.1. Безпроводова сенсорна мережа.

З цього вимоги до пропускної здатності передачі даних і ємності постійно зростають. Підвищення пропускної спроможності може бути досягнуто за рахунок збільшення числа базових станцій, ширини смуги частот радіоканалів або числа радіоканалів, а також підвищення спектральної ефективності. Найбільш економічно виправданим є шлях підвищення

ефективності використання радіочастотного спектру. Заходи пропускної здатності системи в одній соті мережі, що припадає на одиницю радіочастотного спектру. Спектральна ефективність може бути підвищена, наприклад, за рахунок: швидкої адаптації системи до характеристик технології бездротового з'єднання, оптимального вибору схем модуляції і кодування, ортогонального частотного мультиплексування і технології багатоантенних систем - MIMO.

Технологія MIMO має на увазі використання декількох антен на передавальній стороні і декількох антен на приймальній стороні і дозволяє значно підвищити пропускну здатність і/або стійкість системи зв'язку в порівнянні з традиційною системою з однієї передавальної і однієї прийомної антенами (SISO) [1]. У загальному випадку структура системи MIMO має в своєму складі M_t передавачів (передаючих антен) і M_r приймачів (приймальних антен). Розглядаючи MIMO-систему $M_t \times M_r$, бачимо що високошвидкісний потік даних розбивається на M_t незалежних послідовностей зі швидкістю $1/M_t$, які потім передаються одночасно з декількох антен, відповідно використовуючи тільки $1/M_t$ первинної смуги частот. Перетворювач потоку даних на передавальному кінці лінії зв'язку перетворює послідовний потік в паралельний, а на приймальному - виконує зворотне перетворення. Для реалізації просторово-часового розділення сигналів в системах MIMO, безліч виходів (випромінюючих антен), здійснює передачу декількома (в загальному випадку - безліччю) шляхами (променями), а приймає це безліч сигналів, як безліч потоків на кілька прийомних антен (рознесених в просторі). Такі засоби радіозв'язку MIMO забезпечують:

- розширення зони покриття радіосигналами згладжування в ній мертвих зон;
- використання декількох незалежних шляхів поширення сигналу, що підвищує ймовірність роботи по трасах, на яких менший вплив завмирань;
- підвищення пропускної здатності ліній зв'язку за рахунок формування фізично різних каналів. Застосування технології MIMO в наземних бездротових системах зв'язку робить її найбільш перспективною для побудови нових високошвидкісних бездротових систем [2].

Особливість БСС полягає в тому, що послаблення сигналу обмежує дальність поширення радіосигналів, тобто, радіочастотний сигнал зникає (зменшується в силі), поки він поширюється через середовище, в той час як вона проходить через перешкоди. Дану проблему може вирішити одне з основних переваг систем MIMO яка полягає у спроможності здійснювати прийом сигналів, що прийшли за різними маршрутами, що завжди супроводжує радіозв'язку. В даній технології застосовуються кілька антен різного роду, налаштованих на одному і тому ж каналі. Кожна антена передає

сигнал з різними просторовими характеристиками. Таким чином, технологія MIMO використовує спектр радіохвиль більш ефективно і без шкоди для надійності роботи. Кожен приймач «прислухається» до всіх сигналів від кожного передавача, що дозволяє робити шляхи передачі даних більш різноманітними. Таким чином, кілька шляхів можуть бути рекомбіновані, що призведе до посилення необхідних сигналів в бездротових мережах.

При використанні сенсорних систем, наприклад, в розумному будинку, підключених через мережу Wi-Fi з'являється проблема, що в кожен момент часу тільки один пристрій може отримувати і відправляти дані, тоді як інші чекають своєї черги. Збільшення числа підключених до однієї мережі клієнтів призводить до зростання часу очікування обслуговування, появи затримок і зниження ефективності використання мережевих ресурсів. В IEEE 802.11ac застосовується технологія MIMO, як і в IEEE 802.11n. Але, якщо в останньому максимальна розмірність MIMO становить 4×4 (паралельно можуть передаватися чотири інформаційних потоки), то IEEE 802.11ac може використовувати MIMO розмірністю до 8×8 . Якщо передача одного інформаційного потоку в смузі 160 МГц відбувається зі швидкістю 866 Мбіт / с, то вісім потоків підвищують швидкість в 8 разів до 6.9 Гбіт/с. IEEE 802.11ac забезпечує можливість одночасної передачі інформації групам клієнтів. В результаті загальна пропускна здатність бездротової мережі збільшується в декілька разів. Однією з сильних сторін пристроїв стандарту IEEE802.11ac, є економне витрачання енергії. У порівнянні з більш ранніми пристроями економія може досягати до 6 разів [3].

У БСС обмеження найчастіше пов'язані з тим фактом, що сенсорні вузли працюють з обмеженим запасом енергії. Наприклад, науковий моніторинг руху льодовиків, можливо, зажадає датчики, які працюють протягом декількох років, а датчики в разі військових дій можуть бути необхідні тільки протягом декількох годин або днів.

За допомогою нових протоколів передачі даних і технології MIMO можна розробити нові вдосконалені версії БСС, які зможуть одночасно більш ефективно взаємодіяти між собою і з базовою станцією, а також довше працювати від вбудованого акумулятора.

Література

1. Бакулин М. Г., Варукина Л. А. Технология MIMO: принципы и алгоритмы. М. : Горячая линия, 2014.
2. Наука і техніка Повітряних Сил Збройних Сил України, 2013, № 2(11).
3. Huang P. Understanding IEEE 802.11ac VHT Wireless // Electronic Design. 2012.

КОМУНІКАЦІЯ З СЕРВІСНИМ РОБОТОМ ПРИ УПРАВЛІННІ МІНІТЕПЛИЦЕЮ

Нідченко І. А., Лисенко О. І.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: nidchenkoilya@gmail.com

COMMUNICATION WITH SERVICE ROBOT DURING THE MANAGEMENT OF MINI-GREENHOUSE

The article describes possible solutions for connecting a service robot with a mini-greenhouse control system. It shows the main functions required to control a mini-greenhouse and the capabilities of a service robot to meet these requirements.

Система мінітеплиці має можливість працювати самостійно по заданому сценарію, але для більшої ефективності вирощування потребує моніторингу та контролю користувачем. Для вирішення цієї задачі використовується сервісний робот – веб-додаток та чат-бот у додатку Telegram – програма, яка може з'ясувати потреби користувача або повідомити необхідну інформацію за допомогою спілкування у текстовому чаті, за допомогою якого користувач матиме можливість відслідковувати поточні та минулі значення для аналізу росту рослин та прийняти необхідні заходи для покращення навколишнього середовища. Якщо користувач не матиме можливості використовувати додаток Telegram він зможе виконати ті самі операції за допомогою веб-додатку, для доступу до якого потрібен лише доступ до мережі Інтернет [1,2,3].

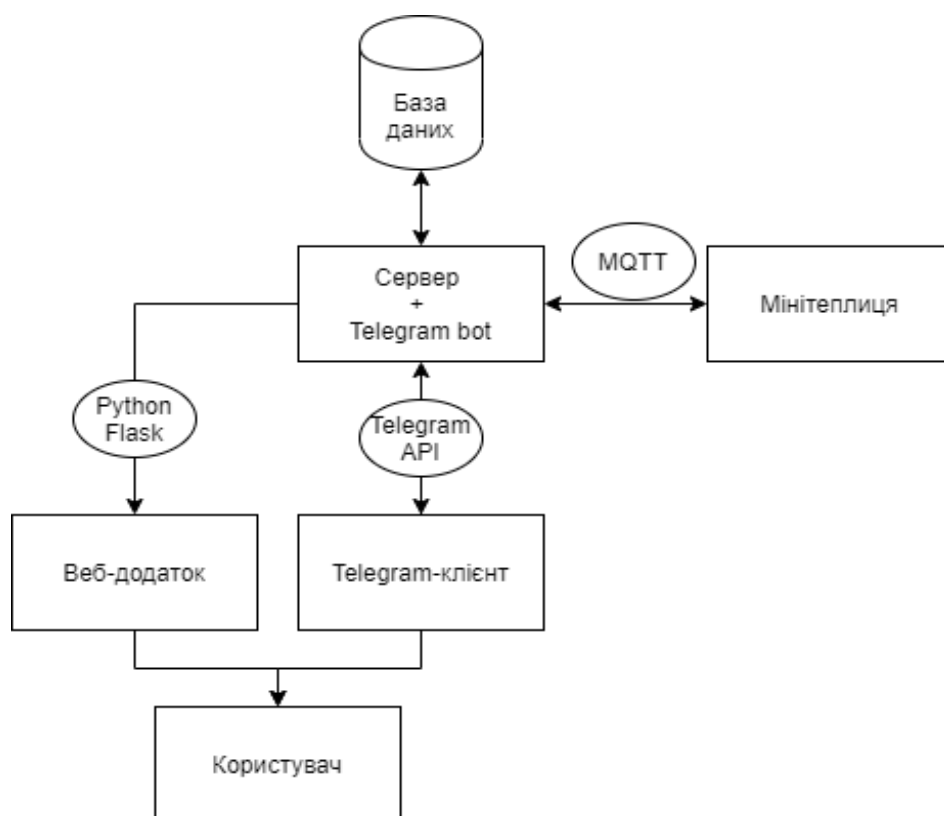


Рис. 1.
Функціональна
блок-схема
інтернет-частини
пристрою.

Контролер мінітеплиці відправляє поточні показники кожні 5 хвилин та постійно слухає команди від клієнта.

MQTT (Message Queue Telemetry Transport) - спрощений мережевий протокол, який працює поверх TCP/IP. Використовується для обміну повідомленнями між приладами за принципом видавець-підписник (pub-sub).

Клієнти підключаються до сервера і відразу після підключення кожен з них здійснює підписку на зацікавлені йому топіки. Все спілкування між клієнтами проходить транзитом через сервер, який перенаправляє дані іншим клієнтам з урахуванням їх підписок.

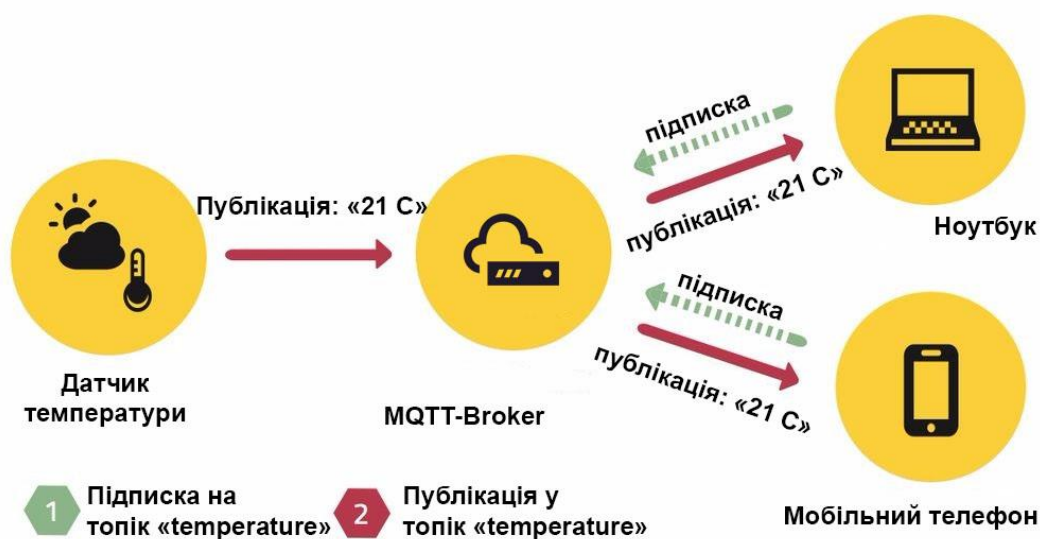


Рис. 2. Принцип роботи MQTT протоколу.

Для роботи усієї Mosquitto системи потрібен брокер – сервер, який буде обробляти запити від клієнтів (мінітеплиць). Водночас цей сервер також буде виступати клієнтом, який зчитує показники пристроїв та відправляє команди від чат-боту.

Сервер у свою чергу обробляє прийняті показники через MQTT, водночас виступаючи брокером-підписником та складає інформацію у свою базу даних. При появі нового запиту від клієнта сервер генерує відповідь через інтерфейс доступу до Telegram боту (або через веб-додаток) та з унікальними даними для поточного клієнта, тобто з інформацією системи, закріпленою за цим клієнтом.

1. Сервісний робот у якості Telegram боту.

Боти - спеціальні акаунти в Telegram, створені для того, щоб автоматично обробляти і відправляти повідомлення. Користувачі можуть взаємодіяти з ботами за допомогою повідомлень, що відправляються через звичайні або групові чати. Логіка бота контролюється за допомогою HTTPS запитів до API для ботів.

За допомогою інтерфейсу розробника для чат-боту налаштовуються шаблони команд для розпізнавання за допомогою яких користувач по запити може отримати поточні показники. Користувач відправляє запит – додаток Telegram розпізнає це як команду та передає на сервер, який генерує відповідь з доступних даних у базі даних та за допомогою API відправляє потрібну клієнту інформацію у форматі чат-боту.

Якщо сервер отримає нові показники від мінітеплиці, які виходять за рамки можливо дозволених – він відправляє повідомлення через чат-бота про необхідність негайного втручання користувача у систему теплиці.

2. Сервісний робот у якості веб-додатку.

Веб-додаток – додаток типу сервер-клієнт, у якому клієнт має можливість взаємодіяти з сервером через браузер. Усі дані при цьому зберігаються на стороні сервера.

При цьому сценарії користувачу не потрібно зайвих додатків на його стороні, він здатний отримати доступ до керування та моніторингу через будь-який веб-браузер. При підключенні нового клієнта сервер генерує графічний інтерфейс з графіками для моніторингу поточних на минулих значень, беручи дані з бази даних.

Висновки. Натурне моделювання підтвердило, що апаратний склад інформаційно-телекомунікаційного забезпечення системи управління мінітеплицею із сервісним роботом у складі мікроконтролерів STM32F303 та ESP8266, датчику температури повітря, вологості та тиску BME280, ємнісного датчику вологості ґрунту, датчику ультрафіолетового світла ML8511 та датчику вуглекислого газу MH-Z19 забезпечує стійке, надійне та ресурсозберігаюче функціонування системи у цілому.

Література

1. Нидченко И. А., Лысенко А. И. Информационно-телекоммуникационная система управления мини-теплицей с использованием сервисного робота. XIV Міжнародна науково-технічна конференція "Перспективи телекомунікацій" ПТ-2020: Збірник матеріалів конференції. К.: КПІ ім. Ігоря Сікорського, 2020. – С. 275-277.
2. Нидченко И. А. Лысенко А. И. Система управления мини-теплицей. Проблемы информатизации: Материалы п'ятнадцятої міжнародної науково-технічної конференції, 9 – 10 квітня 2020 року. - Київ : НАУ, НТУ; Полтава: ПНТУ; Катовице: КЕУ; Париж: Університет Париж VII Венсент-Сен-Дені; Вільнюс: ВДТУ; Харків : ХНДІТМ: Білорусь: БДАЗ, 2020. – С. 106.
3. Нидченко И. А., Лысенко А. И. Информатизация процесса управления мини-теплицей. V - Міжнародна науково-практична конференція «Відкриті еволюціонуючі системи», 19 - 21 травня 2020 р, Таврійський національний університет імені В. І. Вернадського . - С.120-122.

МОДЕЛЬНІ ІГРОВІ ЗАДАЧІ ДЛЯ СИСТЕМ ЛІНІЙНИХ РІВНЯНЬ З ДРОБОВИМИ ПОХІДНИМИ КАПУТТО І РІМАНА-ЛІУВІЛЯ

Руренко О.Г.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: a.rurenko@gmail.com

THE FRACTIONAL GAME PROBLEM FOR THE LINEAR SYSTEMS WITH FRACTIONAL DERIVATIVES IN SENSE OF RIEMANN-LIOUVILLE AND CAPUTO

The fractional game problem is obtained from the classical equation for linear relaxations and oscillations by replacing the first-order derivative and the second-order time derivative by fractional derivative of order α with $0 < \alpha < 2$. It is shown that that presentation of solutions of linear systems with fractional derivatives in sense of Riemann-Liouville and Caputo can be expressed in terms of the matrix Mittag-Leffler functions.

В роботі вивчаються модельні ігрові задачі в конфліктних умовах для систем рівнянь з фрактальними похідними Капутто і Рімана-Ліувіля. Отримано в явному вигляді розв'язки таких систем рівнянь для дробових похідних Капутто і Рімана-Ліувіля порядку $0 < \alpha < 2$.

В n - вимірному евклідовому просторі R^n розглядається процес $z(t)$, $z(t) \in R^n$ у вигляді моделі динамічної гри з двома гравцями, які протидіють один одному через свої керування $u \in U$, $v \in V$, деяка функція $\varphi(u, v)$, $\varphi : U \times V \rightarrow R^n$ описує блок керування, а еволюція гри задана системою диференціальних рівнянь дробового порядку α , $m - 1 < \alpha \leq m$

$$D^\alpha \left(z(t) - \sum_{k=0}^{m-1} \frac{t^k}{k!} z^{(k)}(0+) \right) = Az(t) + \varphi(u, v) \quad (1)$$

з початковими умовами:

$$z^{(k)}(0+) = c_k, k = 0, 1, 2, \dots, m - 1 \quad (2)$$

де A - квадратна матриця порядку n .

Окрім еволюції процесу в просторі R^n задана деяка множина M^* , яку в задачах переслідування-зустрічі називають термінальною. З геометричних представлень динаміки зближення двох конфліктно-керованих процесів в R^n множина M^* вибрана у вигляді:

$$M^* = M_0 + M, \quad (3)$$

де M_0 -лінійний підпростір, а M -деякий компакт із ортогонального доповнення L до M_0 в R^n .

Перший гравець вибирає керування $u(t) \in U$ і має за мету вивести траєкторію процесу $z(t)$ на термінальну множину M^* за мінімальний час, а другий - керування $v(t) \in V$ вибирає таким чином, щоб не допустити "зустрічі" з термінальною множиною, або максимально "відкласти зустріч".

Для цілого m , і дробового α , $m - 1 < \alpha \leq m$ визначені дробовий інтеграл Рімана - Ліувіля порядку β [1] від функції $z(t)$, $t \geq 0$:

$$J^\beta z(t) := \frac{1}{\Gamma(\beta)} \int_0^t (t - \tau)^{\beta-1} z(\tau) d\tau, \quad t > 0,$$

де $\Gamma(\beta)$ - гамма-функція Ейлера, похідна $D^m = \frac{d^m}{dt^m}$ і дробова похідна Рімана-Ліувіля

$$D^\alpha z(t) := D^m J^{m-\alpha} z(t) = \frac{1}{\Gamma(m-\alpha)} \frac{d^m}{dt^m} \int_0^t (t - \tau)^{m-\alpha-1} z(\tau) d\tau.$$

В роботах [2], [3], [4] вивчалися ігрові задачі для систем лінійних рівнянь з дробовими похідними Рімана - Ліувіля і Капутто для $0 < \alpha < 1$ і отримано явні формули для представлення еволюції гри (1), (2) у вигляді:

$$z(t) = E_{\alpha,1}(At^\alpha)c_0 + \int_0^t (t - \tau)^{\alpha-1} E_{\alpha,\alpha}(A(t - \tau)^\alpha) \varphi(u(\tau), v(\tau)) d\tau.$$

Тут $E_{\alpha,\beta}(A)$ - спеціальна матрична функція Міттаг - Леффлера від A

$$E_{\alpha,\beta}(A) := \sum_{k=0}^{\infty} \frac{A^k}{\Gamma(\alpha k + \beta)}, \alpha > 0, \beta \in \mathbb{C},$$

де A - довільна квадратна матриця порядку n з комплекснозначними елементами.

Дана робота є логічним продовженням результатів, які викладені у [2], [3], [4] на більш загальний випадок значень α коли $0 < \alpha \leq 1$ і $1 < \alpha \leq 2$.

Для дослідження ігрових задач з дробовими похідними типу (1), (2), (3) використовується розроблений і добре відомий в теорії диференціальних ігор та розширений для більш широких класів ігрових задач апарат розв'язувальних функцій, який для даного класу ігор системно викладений в роботі [3].

Суть методу полягає в побудові спеціальної числової функції $\alpha(t, \tau, v)$, яка є інтегральною кількісною мірою ступені зближення траєкторії $z(t)$ з термінальною множиною M^* і дозволяє в окремих випадках визначити достатні умови зближення траєкторії $z(t)$ з термінальною множиною M^* .

Література

1. A. Kilbas, H. Srivastava and J. Trujillo, Theory and Applications of Fractional Differential Equations. Amsterdam: Elsevier, 2006.
2. S. Eidelman, A. Chikrii, A. Rurenko, Game Problems for Fractional Systems //Доп. НАН України. –1999. –№1. –С.92-96.
3. A. Chikrii and S. Eidelman "Generalized Mittag-Leffler matrix functions in game problems for evolutionary equations of fractional order Cybern. Syst. Analysis, vol. 36, no. 3, pp. 315-338, 2000.
4. A. Chikrii and I. Matichin, "Presentation of solutions of linear systems with fractional derivatives in the sense of Riemann-Liouville, Caputo and Miller-Ross J. Autom. Inf. Sci., vol. 40, no. 6, pp. 1-11, 2008.

АНАЛІЗ ЗАСТОСУВАННЯ МЕТОДІВ МАРШРУТИЗАЦІЇ В AD HOC МЕРЕЖАХ ІЗ БПЛА

Валуйський С.В., Єфименко О.С.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: o.yefymenko@gmail.com

ANALYSIS OF THE ROUTING METHODS APPLICATION IN AD HOC NETWORKS WITH UAVS

The article describes the result of the analysis of existing data transmission protocols in UAV networks. Features of protocols, their influence on a bandwidth, a data transmission delay, fault tolerance of a system and energy efficiency of network nodes are considered.

Мережі БПЛА, що призначені для різних застосунків, можуть варіюватися від повільних динамічних систем до тих, що змінюють своє місце розташування з великою швидкістю. Одні вузли мережі можуть вийти з ладу через збій в системі або втрату живлення, інші можуть приєднуватися динамічно. У енергоефективних мережах радіопристрої можуть бути автоматично вимкнені для економії енергії при відсутності навантаження та відсутності активних з'єднань.

До таких мереж висуваються суворі вимоги, такі як: пошук найбільш ефективного маршруту, що дозволяє мережі масштабуватись з мінімальними затримками, піклуючись про мобільність та забезпечуючи високу якість обслуговування.

Для ефективної маршрутизації в БПЛА мережах необхідна постійно оновлювана інформація про місцезнаходження вузлів мережі, контроль заряду безпілотних апаратів, стійкість до розривів зв'язку та зміни топології. Проектування мережевого рівня для мереж БПЛА залишається одним із найскладніших завдань [1].

Статичні протоколи мають статичні таблиці маршрутизації, які обчислюються та завантажуються під час запуску задачі. Ці таблиці не можуть змінюватися під час функціонування. Через це обмеження ці системи не є стійкими до несправностей та непридатні для динамічно змінюваного середовища. Їх застосовність в мережах БПЛА обмежена.

Проактивні протоколи використовують таблиці маршрутизації для зберігання інформації про всі хости мережі. Таблиці повинні оновлюватися при зміні топології. Основна перевага проактивних протоколів – найбільш актуальна інформація про топологію та хости мережі. Але для застосування таких протоколів в мережах БПЛА таблиці повинні оновлюватися шляхом передачі інформації між вузлами мережі, що робить це поганим вибором для

БПЛА мереж через малу пропускну здатність каналів зв'язку [2].

Реактивні (On-demand) протоколи – це протоколи по запиту. Маршрут між вузлами зберігається тільки тоді, коли між ними відбувається передача даних. Реактивні протоколи створені на заміну проактивним. Завдяки активації по запиту, смуга пропускання не завантажується періодичним обміном інформації про топологію мережі та її хости. Але недоліком є час, необхідний для пошуку маршруту між хостами мережі під час сеансу зв'язку, що створює додаткові затримки [3].

Реактивні протоколи поділяються на два типи:

- Маршрутизація джерела;
- Перехідна маршрутизація.

В першому типі всі пакети мають інформацію про хост, що відправив пакет, та вузол призначення, проміжні хости можуть пересилати ці пакети в відповідності до таблиці маршрутизації.

В реактивних протоколах з перехідною маршрутизацією пакети зберігають інформацію тільки про місце призначення. Такі протоколи мають перевагу в мережах з частою зміною топології, проміжні хости можуть пересилати пакети у відповідності з отриманою інформацією.

Гібридні протоколи. Затримка при пошуку маршруту в реактивних протоколах та заповнення каналу зв'язку для оновлення таблиць маршрутизації в проактивних протоколах – ці недоліки можуть бути усунені. Вузли мережі об'єднані в структурні одиниці – зони, що обумовлені географічним розташуванням вузлів. Трафік, в першу чергу, передається між зонами, що зменшує необхідність будувати маршрут між великою кількістю хостів та значно знижує затримки в мережі [2].

Географічні 3D протоколи. Особливістю таких протоколів є те, що хост-джерело має інформацію про географічне розташування хоста-приймача, що дає можливість відправляти інформацію, базуючись на координатах, без побудови маршруту між хостами мережі. Технологія заключається в тому, що кожен вузол мережі пересилає пакети до наступного хоста, який розташований ближче, до місця призначення. Недоліком таких протоколів є затримка, яка виникає, коли останній хост не може надіслати інформацію далі. В такому випадку запускається механізм відновлення, інформація передається на інший вузол мережі [3].

Деталі порівняльного аналізу розглянутих протоколів маршрутизації наведено в Табл.1. Протоколи усіх типів недостатньо ефективні в мережах на основі БПЛА, а отже потребують вдосконалення, що буде розглянуто в подальших дослідженнях.

Таблиця 1. Нюанси використання існуючих протоколів в БПЛА мережах.

Протокол	Нюанси застосування в БПЛА мережах
Статичні (LCAD, MLHR, Data Centric)	Фіксовані таблиці, які не підходять для динамічної топології, не масштабуються, мають більшу вразливість до помилок оператора, мають великі затримки.
Проактивні (OLSR, GSR, FSR, DSDV, BABEL, B.A.T.M.A.N)	Великі витрати на постійне оновлення таблиць, неможливість використання в мережах з обмеженою пропускнуою здатністю, повільна реакція на зміну топології призводить до затримок.
On-demand or reactive (DSR, AODV)	Висока затримка при пошуку маршруту. Маршрутизація джерела даних погано масштабується. Через великий розмір заголовків збільшується затримка.
Гібридні (ZRP, TORA)	Важко застосувати в мережах з динамічною топологією.
Географічні 3D (GHG, GRG, GDSTR-3D, MDT)	Недоліком є статична топологія мережі. Періодично неможливо отримати інформацію про розташування вузлів мережі. Механізм відновлення неефективний через відсутність побудованого маршруту.

Література

1. I. Bekmezci, O. K. Sahingoz, S. Temel, "Flying Ad-Hoc Networks (FANETs): A survey," Ad Hoc Networks, 2013.
2. K. Daniel, C. Wietfeld, "Using Public Network Infrastructures for UAV Remote Sensing in Civilian Security Operations," Homeland Security Affairs, Best Papers from the IEEE Conference on Technologies for Homeland Security, Jan 2011, <http://www.hsaj.org/?article=0.3.3> Access date: Oct 2014.
3. P. B. Bök, Y. Tuchelmann, "Context-Aware QoS Control for Wireless Mesh Networks of UAVs," Proceedings of the International Conference on Computer Communications and Networks (ICCCN), Aug 2011.

ПІДХОДИ ДО ЕНЕРГОЗБЕРЕЖЕННЯ В БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ

Кучеренко А.А.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: ns.kycheryashka@gmail.com

APPROACHES TO ENERGY SAVING IN WIRELESS SENSOR NETWORKS

The main approaches to energy saving in wireless sensor networks are considered. This is a very broad topic because energy, as one of the most important resources in wireless networks, needs to be widely managed to extend network life. To address this issue, several research papers have been conducted leading to various schemes as well as protocols.

Розглянуто основні підходи до енергозбереження в бездротових сенсорних мережах. Це дуже широка тема, оскільки енергією, як одним з найбільш важливих ресурсів в мережах бездротової мережі, необхідно широко управляти, щоб продовжити термін служби мережі. Для вирішення цього питання було проведено кілька дослідницьких робіт що призводить до різних схем, а також протоколів.

У бездротових сенсорних мережах є кілька проблем, більшість з яких призводить до втрати енергії [1]. У цьому розділі висвітлено основні причини втрати енергії у зв'язку з бездротовими датчиками.

- Прослуховування в режимі очікування: відбувається, коли вузли прокидаються і прослуховують вхідні кадри, навіть коли дані не передаються. Це вичерпує термін служби бездротових сенсорних мереж.

- Зіткнення: виникає, коли дві або більше близьких станцій хочуть передавати пакети одночасно. Коли це трапляється, усі пакети, що беруть участь у зіткненні, повинні бути відкинуті та повторно передані, що призводить до втрат енергії.

- Надмірний слух: коли бездротовий канал транслює повідомлення, багато вузлів навколо відправника можуть підслухати пакетну передачу, навіть коли вони не є призначеними одержувачами цих передач. Підслуховування непотрібного трафіку може призвести до втрати енергії.

- Накладні витрати на контрольний пакет: контрольні пакети витрачають багато енергії на передачу прийому та прослуховування, тому бажано використовувати меншу кількість контрольних пакетів для передачі даних, щоб зменшити накладні витрати.

Енергія є одним з найбільш важливих ресурсів для бездротових сенсорних мереж, але однією із загальних проблем більшості цих WSN є відсутність надійного живлення для кожного вузла датчика в мережі.

Розбивка енергії, споживаної в мережі, залежить від конкретного вузла датчика. По суті, передача даних споживає набагато більше енергії, ніж обробка даних. Однак енергія, споживана сенсорною підсистемою, змінюється залежно від кожного вузла. У деяких випадках зондування споживає менше енергії, ніж ті, що потрібні для обробки даних, тоді як в інших випадках воно навіть споживає більше енергії, необхідної для передачі даних [2].

З огляду на вищесказане, було проведено кілька дослідницьких робіт для вирішення енергетичної проблеми, результатом якої є різні схеми та протоколи.

Ці схеми та протоколи можна згрупувати таким чином:

- робочий цикл,
- керований даними,
- на основі мобільності.

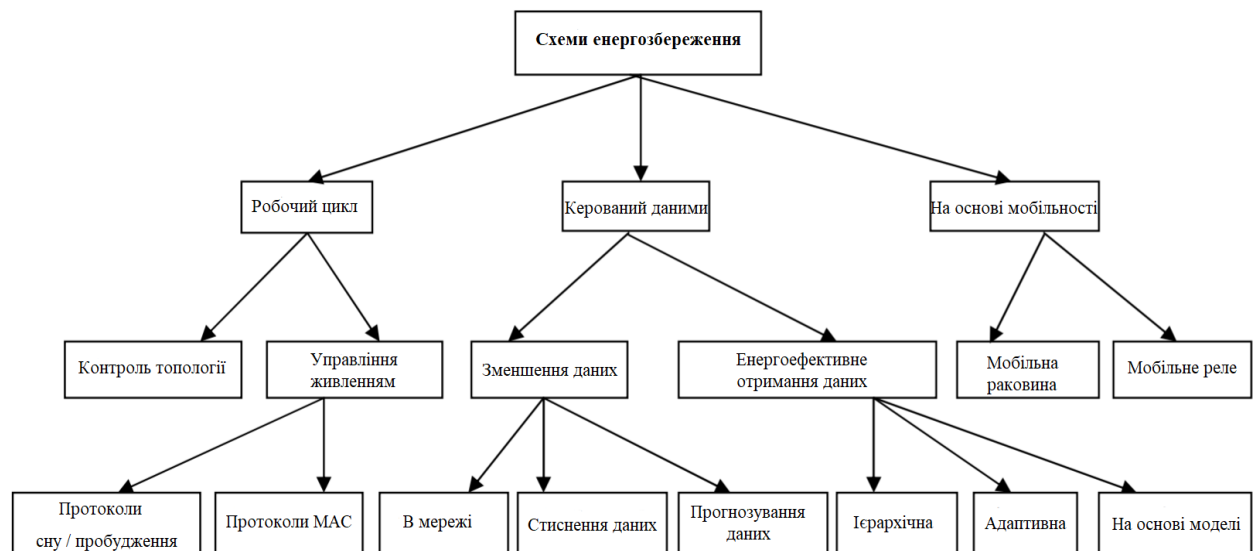


Рис. 1. Схеми та протоколи енергозбереження.

1. Робочий цикл.

У радіоприймачах датчиків вузлів існують різні режими: активний і режим сну. Вузли перемикаються між обома режимами на основі діяльності мережі, і така поведінка відома як робочий цикл. Під час простою було виявлено, що енергія простою дуже важлива для економії енергії в бездротових сенсорних мережах. Таким чином, робочий цикл можна визначити як відсоток часу активності вузла протягом свого життя.

2. Підхід, керований даними [3].

Існує два шляхи, за допомогою яких підхід, керований даними, впливає на споживання енергії :Спочатку він сортує непотрібні зразки, що призводить до марного споживання енергії та зупиняє їх передачу до

раковини. По-друге, це мінімізує енергоспоживання сенсорної підсистеми, підтримуючи точність датчика на розумному рівні.

Перший вирішив проблему непотрібних зразків, тоді як другий зменшує енергію, що витрачається на сенсорну підсистему.

3. Підхід на основі мобільності.

Мобільність може бути використана як засіб для зменшення споживання енергії в ситуаціях, коли деякі вузли датчиків є мобільними. Мобільність вузлів датчиків може бути досягнута різними способами: По-перше, до датчика може бути прикріплений мобілізатор, який допомагає змінити його розташування; однак цей рух обмежений кількома вузлами, які не стримуються енергією. Іншим методом є встановлення датчиків на мобільні елементи, такі як тварини та машини. Цього можна досягти, поставивши всі датчики на мобільні елементи, щоб зробити всі вузли мобільними, або розмістивши лише кілька спеціальних вузлів на мобільному елементі, тоді як інші статичні. Схеми енергозбереження на основі мобільності можна класифікувати залежно від природи мобільного елемента, яким є мобільна раковина (MS) або мобільне реле (MR).

Більшість схем жертвували однією чи кількома речами задля економії енергії. Одним з таких є алгоритм зменшення даних, який оптимізує компроміс між економією енергії та достовірністю даних. Подібним чином протокол керування живленням Appsleep та мобільна ретрансляційна система MULE обмінювали затримки енергії, що обмежує їх застосування в системах реального часу. Підхід управління топологією торгує пропускнуою здатністю для збільшення енергозбереження, тоді як мобільна раковина максимізує термін служби бездротової сенсорної мережі, допускаючи значний рівень затримки. Ці обмеження потребують подальшого дослідження та вдосконалення, щоб підвищити ефективність схем.

Незважаючи на велику кількість досліджень у галузі енергозбереження в бездротових сенсорних мережах, все ще існують інші сфери, які необхідно повністю використати для вирішення проблеми енергозбереження. Одним з таких є збирання енергії з навколишнього середовища не тільки як джерела енергії, а й як засіб збереження енергії в бездротових сенсорних мережах.

Література

1. Ye W. & Heidemann J. (2003) "Medium Access Control in Wireless Sensor Networks" Technical Report ISITR-580, USC/Information Sciences Institute.
2. Demirkol I., Ersoy C., & Alagöz F. (2006), "MAC Protocols for Wireless Sensor Networks: A Survey" IEEE Communications Magazine, pp 115 – 121.
3. Lai S. (2010), "Duty-Cycled Wireless Sensor Networks: Wakeup Scheduling, Routing, and Broadcasting" a thesis submitted to Virginia Polytechnic Institute and State University.

РОЗВИТОК МЕТОДУ МАРШРУТИЗАЦІЇ В БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ НА ОСНОВІ ЗАСТОСУВАННЯ АЛГОРИТМУ ВИБОРУ ГОЛОВНИХ КЛАСТЕРНИХ ВУЗЛІВ

Осинський А.К., Лисенко О.І.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: toni02133@gmail.com

DEVELOPMENT OF ROUTING METHOD IN WIRELESS SENSOR NETWORKS BASED ON THE APPLICATION OF MAIN CLUSTER NODES SELECTION ALGORITHM

The article describes the main advantages and problems of the routing method in wireless sensor networks using the algorithm for selecting the main cluster nodes.

У статті описано основні переваги та недоліки методу маршрутизації в бездротовій мережі сенсорні мережі з використанням алгоритму вибору основних вузлів кластера.

При використанні кластеризації в кожному кластері вибираються головні кластерні вузли (ГКВ), які служать для збору даних з вузлів кластера і передачі їх до базової станції. ГКВ може бути обраний вузол з будь-яким рівнем залишкової енергії, в тому числі з мінімальним. Однак велика кількість головних вузлів, що мають низьку енергію, здатне привести до відмови мережі. Саме тому характеристика ГКВ визначає продуктивність кластера і всієї БСМ в цілому, а вибір головного кластерного вузла грає істотну роль у функціонуванні сенсорних мереж.

Математична модель прогнозування споживання енергії.

Розглянемо модель, запропоновану Jin Shyan Lee і ін. [1], в якій не береться до уваги споживання енергії вузлами, що перебувають в режимах простою або сну. У даній моделі передбачається, що кожен вузол посиляє l біт даних на вузол на відстань d , маючи запас енергії E_3 і споживаючи кількість енергії $E_{\text{пд}}$ для передачі даних, яка задається як вираз:

$$E_{Tx} = \begin{cases} l * E_3 + l * \varepsilon_{\text{в.п.}} * d^2, & d < d_0, \\ l * E_3 + l * \varepsilon_{\text{б.п.}} * d^4, & d \geq d_0, \end{cases} \quad (1)$$

де $\varepsilon_{\text{в.п.}}$ - фактор, що впливає на енергоспоживання для моделі вільного простору; $\varepsilon_{\text{б.п.}}$ - фактор, що впливає на енергоспоживання для моделі багатоколінійні поширення хвиль; d_0 - порогове значення.

Граничне значення d_0 може бути задано наступним чином:

$$d_0 = \sqrt{\frac{\varepsilon_{\text{в.п.}}}{\varepsilon_{\text{б.п.}}}}. \quad (2)$$

Залежно від відстані d використовується або модель вільного простору, або модель багатоколійного загасання каналу. Енергія, необхідна кожному вузлу для прийому даних $E_{\text{пр}}$, визначається як

$$E_{\text{пр}} = l * E_3 . \quad (3)$$

Ця модель обчислює енергію передачі $E_{\text{пд}}$ і прийому $E_{\text{пр}}$ вузла, не враховуючи роль вузла в кластері, тобто без урахування, що він є головним кластерним вузлом або членом кластера.

Виконання вузлами ролей головного кластерного вузла або члена кластера змінюється в залежності від їх завдань. Отже, споживання енергії ГКВ $E_{\text{ГКВ}}$ і його членами $E_{\text{чк}}$ може бути обчислено незалежно один від одного шляхом модифікації виразів (1) і (2), з урахуванням частоти повторюваних зв'язків сенсорного вузла. $E_{\text{ГКВ}}$ і $E_{\text{чк}}$ обчислюються наступним чином:

$$\begin{aligned} E_{\text{ГКВ}} &= E_{\text{прБС}} + (E_{\text{прчк}} + E_{\text{пдчк}} * m) + E_A + E_{\text{пдБС}} , \\ E_{\text{чк}} &= E_{\text{прГКВ}} + E_{\text{пдГКВ}} \end{aligned} \quad (4)$$

де $E_{\text{прБС}}$ - енергія, споживана ГКВ при прийомі повідомлень від базової станції; $E_{\text{прБС}}$ - енергія, споживана ГКВ при передачі агрегованих даних до базової станції; $E_{\text{прчк}}$ - енергія, споживана ГКВ при прийомі даних від членів кластера; $E_{\text{пдчк}}$ - енергія, споживана ГКВ при передачі повідомлень членам кластеру; E_A - енергія, споживана ГКВ при агрегації даних; m - кількість вузлів в кластері; $E_{\text{прГКВ}}$ - енергія, споживана вузлом при прийомі повідомлень від ГКВ; $E_{\text{пдГКВ}}$ - енергія, витрачена вузлом для передачі даних від вузла до ГКВ.

Метод вибору головного кластерного вузла [2-5].

У загальному випадку енергія ГКВ та членів кластера БСМ витрачається в процесі зондування, обробки даних і взаємних обмінів інформацією. Таким чином, коли значення рівня енергії ГКВ стає менше порогового значення, даний ГКВ перестає бути головним, що призводить до перевиборів ГКВ. У подібних випадках у вузла, часто взаємодіє з іншими вузлами кластера, виникає ймовірність стати ГКВ огляду на високий рівень його залишкової енергії в поточний момент часу. Однак в цьому полягає істотний недолік: оскільки енергія вузла, залученого в постійний обмін даними з сусідніми вузлами, буде швидко виснажуватися в порівнянні з вузлами, що обмінюються даними набагато рідше, це буде приводити до частих перевиборів ГКВ. З іншого боку, якщо споживання енергії ГКВ та членами кластера може бути передбачене на основі їх попередніх сеансів зв'язку, то інтервал перевиборів ГКВ можна таким способом збільшити. Щоб вирішити це завдання, пропонується метод вибору ГКВ БСМ, заснований на нечіткій логіці. На рис. 1 представлена модель нечітко керуємої системи для вибору ГКВ. Вхідними параметрами є залишкова енергія вузлів (RE), щільність

розподілу сусідніх вузлів в кластері (ND) і централізованість вузла (NC), а вихідним параметром - ймовірність вибору ГКВ (CHS).

Лінгвістичні змінні RE і ND приймають значення «Низька», «Середня», «Висока», а змінна NC - «Близько», «Середньо», «Високо». На рис. 3-5 наведені функції належності вхідних параметрів системи. На основі знань про лінгвістичної змінної використовуються 27 правил нечіткої логіки для прийняття.

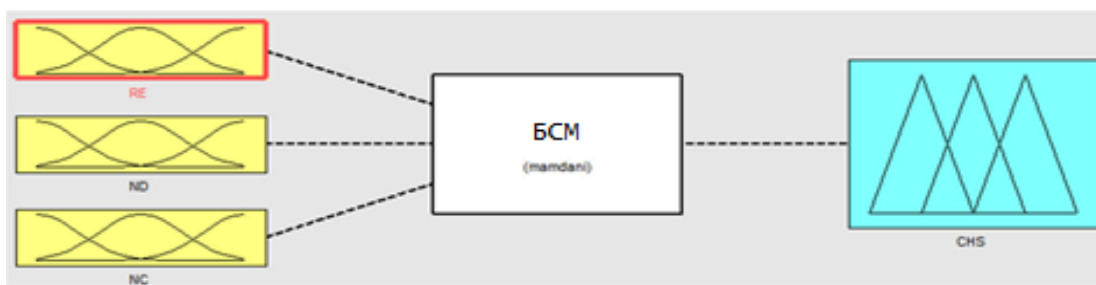


Рис. 2. Модель нечітко керуємої системи.

Чим ближче значення вихідного параметра буде до одиниці, тим вище ймовірність у вузла стати ГКВ в БСМ. Пропонована система нечітких правил приймає рішення, засноване на трьох основних параметрах відповідно до заздалегідь заданої базою правил, наведеної в таблиці.

Висновки. Результатом дослідження став алгоритм вибору ГКВ БСМ з використанням нечіткої логіки. У запропонованій системі використовуються такі параметри, як залишкова енергія вузлів БСМ, щільність розподілу сусідніх вузлів в кластері і централізованість вузла. Алгоритм реалізований з використанням програмного пакету MATLAB. Результати моделювання показують, що використання перерахованих вище вхідних параметрів дозволяє робити оптимальний вибір ГКВ, що, в свою чергу, робить позитивний вплив на енергоефективність БСМ. Надалі планується дослідити вплив більшої кількості вхідних параметрів на ймовірність вибору ГКВ сенсорної мережі, що визначає продуктивність системи в цілому.

Література

1. Lee J. S., Cheng W.-L. Fuzzy-Logic-Based Clustering Approach for Wireless Sensor Networks Using Energy Predication // IEEE Sensors Journal. 2012. Vol. 12, no.
2. Yan Gu, Yucheng Shao, Han Han, Tong Yi. A Clustering Routing Algorithm of WSN based on Uneven Nodes Deployment // IEEE International Conference on Wireless Communications and Signal Processing (WCSP), 2011. P. 1–6.
3. Singh A. K., Purohit N., Varma S. Fuzzy Logic based Clustering in Wireless Sensor Networks: A Survey // International Journal of Electronics. 2012. Vol. 100, iss. 1. P. 126–141.
4. Lee J. S., Cheng W.-L. Fuzzy-Logic-Based Clustering Approach for Wireless Sensor Networks Using Energy Predication // IEEE Sensors Journal. 2012. Vol. 12, no. P. 2891–2897.
5. Young-Long Chen, Wei-Hsiang Huang. Fuzzy Logical Control with Taguchi Method for Cluster Heads Election in Wireless Sensor Networks // IEEE International Symposium on Computer, Consumer and Control, 2012.

СИНХРОНІЗАЦІЯ ЧАСУ В БЕЗПРОВІДНИХ СЕНСОРНИХ МЕРЕЖАХ

Синявіна Є.П.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: janesynavina13@gmail.com

TIME SYNCHRONIZATION IN WIRELESS SENSOR NETWORKS

This article explains the time synchronization problem in wireless sensor networks and details the basic algorithms proposed in this area. Wireless sensor networks consist of small devices distributed over geographical area. Each one of these devices has sensing, computing, and communicating components. Wireless sensor networks are used in many applications where partial or full time synchronization in the network is required. Time synchronization aims at equalizing the local times for all nodes in the network, if necessary.

Бездротова мережа складається з просторово розподілених автономних пристроїв для спільного моніторингу фізичних або екологічних умов, таких як температура, звук, вібрація, тиск, рух та забруднюючі речовини, в різних місцях. Сенсорні мережі - це особливий тип спеціальних мереж, де бездротові пристрої (зазвичай їх називають вузлами в мережі) працюють разом, щоб спонтанно формувати мережу без потреби в будь-якій інфраструктурі [4]. Вузли можуть надсилати дані, отримувати дані або діяти як маршрутизатори в мережі.

Традиційні методи синхронізації, які використовувались у дротових мережах, не підходять для бездротових мереж. NTP, який широко використовується в Інтернеті, занадто складний для впровадження та не є енергоефективним. GPS, з іншого боку, не є практичним, оскільки пристрій, який потрібно підключити до вузла мережі, є великим і дорогим. Крім того, оскільки датчики зазвичай використовуються в суворих умовах, сигнали GPS часто недоступні.

Обмін повідомленнями використовується в багатьох алгоритмах синхронізації часу. Якщо один вузол відправляє пакет із позначкою часу, недетерміновані затримки, такі як час доступу та розповсюдження, ускладнюють для вузла приймача точну синхронізацію з вузлом відправника.

Загалом, наступні елементи сприяють **помилкам синхронізації** [3]:

- *Час надсилання*: це загальний час побудови повідомлення та передачі його в мережевий інтерфейс, який потрібно надіслати (залежить від налаштувань ОС).
- *Час доступу*: це час, необхідний для доступу до фізичного каналу передачі.
- *Час поширення*: це час, необхідний для розповсюдження повідомлення по повітрю від мережевого інтерфейсу відправника до мережевого інтерфейсу приймача.
- *Час отримання*: це час, витрачений на отримання повідомлення через мережевий інтерфейс та його передачу на прикладний рівень хосту.

При розробці алгоритму синхронізації часу обмеження бездротової мережі забезпечують виконання певних вимог. Зазвичай для оцінки будь-якої техніки синхронізації використовують такі показники: точність, надійність, масштабованість, довговічність, енергоефективність, вартість, сфера застосування, затримка.

Методи синхронізації для безпроводних сенсорних мереж.

Схеми синхронізації спрямовані на коригування місцевого часу вузлів мережі до одного і того ж еталонного значення. Найбільш суворі та енергоємні схеми вимагають синхронізації всіх вузлів у мережі постійно (завжди увімкнено), тоді як інші більш спокійні схеми вимагають синхронізації кількох вузлів одночасно.

А. Довідкова синхронізація трансляції (Reference Broadcast Synchronization, RBS). У [1] було введено RBS, де приймач із приймачем замість відправника з приймачем використовується синхронізація. Вузли, що транслюють маяки, та інші вузли використовують час прибуття цих маяків як посилення, щоб знаходити часові зсуви між ними. Основна ідея цього алгоритму полягає у видаленні недетермінованого часу надсилання. Єдині джерела помилок у цій схемі зумовлені недетермінованістю розповсюдження та часом прийому. Помилками, спричиненими часом поширення, можна знехтувати, якщо припустити, що радіодіапазон короткий і що маяк транслюється на всі вузли в цей час. Тож час отримання - це єдине джерело помилок у цій схемі.

Типовий сценарій зв'язку полягає в тому, що один вузол надсилає маяк своїм сусідам, і приймачі обмінюються часом отримання цього маяка, щоб знайти їх відносні часові зсуви, а отже, синхронізувати між собою. За допомогою цієї техніки можна досягти точності в декілька мкс. Крім того, цей алгоритм був застосований до машин Linux, що здійснюють зв'язок за протоколом 802.11, і була досягнута точність $6,29 \pm 6,45$ мкс.

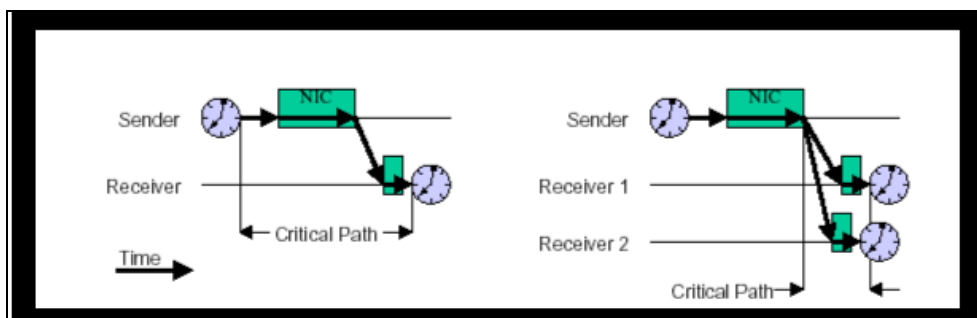


Рис. 1. Аналіз критичного шляху для традиційних протоколів синхронізації часу (ліворуч) та RBS (праворуч) [1].

В. Протокол синхронізації таймінгів для сенсорних мереж (Timing-Sync Protocol for Sensor Networks, TPSN) запропоновано в [5]. Ця техніка синхронізації складається з двох фаз; фаза виявлення рівня та фаза синхронізації.

1. На *фазі виявлення* кожному вузлу присвоюється рівень; лише одному вузлу присвоюється рівень 0, і він називається кореневим вузлом.

2. На другій фазі вузол рівня n синхронізується з вузлом рівня $n-1$, і до кінця цієї фази досягається загальномерева синхронізація. Знову ж таки, кореневий вузол починає *фазу синхронізації*, надсилаючи пакет `time_sync`. Вузол A рівня n синхронізується з вузлом B рівня $n-1$ за допомогою двостороннього обміну повідомленнями. Вузол A відправляє пакет разом із місцевим часом передачі T_1 .

Вузол В приймає пакет в момент часу T_2 , який можна обчислити як [5]:

$$T_2 = T_1 + T_d + \Delta \quad (3)$$

де T_d є затримкою розповсюдження, а Δ є відносним зміщенням тактової частоти між вузлами, і обидва вважаються постійними протягом часу обміну повідомленнями. Вузол В чекає випадковий час і відповідає назад на вузол А через пакет підтвердження в момент T_3 , який включає значення T_1 , T_2 , T_3 і номер його рівня. Як тільки вузол А отримає цей пакет в T_4 , він може обчислити Δ і T_d наступним чином [5] і синхронізуватися з вузлом В.

$$\Delta = \frac{(T_2 - T_1) - (T_4 - T_3)}{2}; \quad T_d = \frac{(T_2 - T_1) + (T_4 - T_3)}{2} \quad (4)$$

Цей метод синхронізації всіх вузлів на рівні n до вузлів на рівні $n-1$ триває до тих пір, поки всі вузли в мережі не синхронізуються.

Порівнюючи TPSN з RBS, TPSN має більше накладних енергетичних витрат, ніж RBS. Пакети, надіслані для вибору кореневого вузла, і ті, що надіслані на фазі виявлення рівня, вважаються накладними витратами. Цей вид накладних витрат скорочує термін служби мережі, особливо якщо кореневі вузли так часто гинуть у мережі, і весь метод синхронізації повинен бути повторений. Ми виявили, що RBS та TPSN працюють дуже добре з точки зору точності. Точність їх становить кілька мікросекунд. Оскільки надсилання та отримання пакетів є найбільш енергоємним завданням при синхронізації мережі, кількість пакетів, необхідних для синхронізації пари вузлів, може бути використана для оцінки енергоефективності.

У RBS, який є алгоритмом від приймача до приймача, 4 пакети надіслані та 3 пакети отримані для синхронізації двох вузлів. У TPSN 2 відправлені та 2 отримані пакети для синхронізації двох вузлів. Незважаючи на те, що TPSN звучить більш енергоефективно, той факт, що для виявлення рівня в TPSN потрібні додаткові відправлені та отримані пакети, і той факт, що більше ніж один приймач може синхронізуватися в одному імпульсі в RBS. Деревовидні алгоритми синхронізації гнучкі, і на основі заданої точності складність може бути як високою, так і низькою. Кореневий вузол відіграє головну роль у цих алгоритмах і може бути підключений до зовнішніх вузлів, щоб отримати реальний час життя.

Література

1. J. Elson, L. Girod, and D. Estrin, "Fine-Grained Time Synchronization using Reference Broadcasts," Proceedings of the Fifth Symposium on Operating Systems Design and Implementation (OSDI 2002), Boston, MA, December 2002.
2. M.L. Sichitiu and C. Veerarittiphan, "Simple, Accurate Time Synchronization for Wireless Sensor Networks," Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE Volume 2, 20-20 March 2003 pps.1266 - 1273 vol.2.
3. S. Ping, "Delay Measurement Time Synchronization For Wireless Sensor Networks," Technical Report, Intel Research Berkeley Lab, 2003.
4. F. Sivrikaya and B. Yener, "Time Synchronization in Sensor Networks: A Survey," Network, IEEE Volume 18, Issue 4, July-Aug. 2004, pps.45 – 50.
5. S. Ganeriwal, R. Kumar, and M. Srivastava, "Timing Sync Protocol for Sensor Networks," ACM SenSys, Los Angeles, November 2003.

ІНФОРМАЦІЙНА ФІЛОСОФІЯ ТЕЛЕКОМУНІКАЦІЙ

Гребенніков В.О.

E-mail: hreben@ukr.net

INFORMATION PHILOSOPHY OF TELECOMMUNICATIONS

The most general principles of the telecommunication sphere in organization, functioning and development in the society are considered. These principles must be followed at carrying out more concrete scientific researches, design works and practical activity in this sphere. To explain and substantiate these principles, the methodology of information philosophy is used, which is based on general physical and biological theories of the origin and role of information in physical and animate nature. New principles of the telecommunication sphere are proposed, aimed at the problems of existential transformation of human societies from the liberal-capitalist development paradigm to the paradigm of sustainable development.

Філософія – це найзагальніша форма знання про принципи і характеристики довколишнього світу – основа світогляду і практичної діяльності людини. Недарма один з наукових ступенів в усіх науках має назву «доктор філософії». Філософські знання у сфері телекомунікацій допомагають у правильній постановці завдань наукової, конструкторської чи практичної діяльності у цій сфері, що оптимізує витрату трудових і матеріальних ресурсів та збільшує суспільну ефективність телекомунікацій.

Більше двох тисячоліть основним способом отримання філософських знань (істин, принципів) були загальні спостереження за природою, суспільствами і людьми, узагальнення цих спостережень у формі коротких мовних формулювань та мовно-логічне доведення істин. За довгу історію філософії, внаслідок суб'єктивізму філософів та під впливом наукового і соціального прогресу людства, цих істин накопичено велику кількість, Філософські істини нерідко суперечать одна одній і своєю сукупністю створюють несистемну, суперечливу картину світу. Багато з цих істин сьогодні стали вже анахронізмом, але більшість їх зберіглася, будучи адаптованими під новий рівень знань людства у останні десятиліття.

Нові відкриття і наукові знання в космології, еволюції живої природи, біохімії та нейрофізіології сьогодні дають можливість створити більш цілісну філософську картину Всесвіту, ролі в ньому живих істот і самої людини. В цій картині Всесвіту важливе місце відводиться інформації, нарівні з матерією і енергією, що системно і переконливо показано в роботах американського астрофізика, «інформаційного філософа» Боба Доулі, наприклад, [1]. Він творчо, з урахуванням найновіших наукових досягнень, розвиває ідеї багатьох філософів про нематеріальну компоненту Всесвіту («ідея і форма» у Платона, «дух» у Гегеля і Ніцше тощо) і вважає, що фізичну основу Всесвіту складають дві матеріальні компоненти – речовина і енергія та нематеріальна компонента – інформація. Саме інформація, на його переконання, є основою різноманітності і порядку в усіх явищах Всесвіту від елементарних часток до зірок, планет і галактик («порядок із хаосу»), основою виникнення і збереження життя на Землі («порядок із порядку») та свідомості і розуму в тваринному світі («чиста інформація із порядку»). Доулі, услід за Норбертом Вінером, підкреслює, що інформація – це не матерія чи енергія, але вона потребує матерії для втілення та енергії для передавання.

Надаючи належної уваги інформаційній компоненті Всесвіту, Доулі успішно аналізує сутність багатьох давніх проблем філософії і фізики та надає їм прості і

переконливі «інформаційні» розв'язки. Його «інформаційно-філософський» підхід до аналізу і пояснення різноманітних проблем і явищ Всесвіту може стати універсальною методологією у проведенні наукових досліджень та виробленні практичних рекомендацій. Цей підхід перегукується із заключним висновком відомого дослідника теорій інформаційного суспільства Френка Уебстера про те, що краще зрозуміти сутність інформатизації суспільства і ролі інформації в сучасному світі можна з'ясувавши: *«якого типу інформація з'явилася, навіщо вона була потрібна, які групи в суспільстві її використали і для яких цілей»* [2]. Логічне узагальнення такого «інформаційно-філософського» підходу вже дало можливість істотно розширити і уточнити базові поняття інформаційної сфери в живій природі і в суспільстві, такі як «інформація» та «інформатизація» [3], синтезувати новий системний погляд на інформаційну сферу суспільства [стаття в процесі публікації]. Є сенс застосувати такий підхід і для дослідження основних (філософських) питань функціонування і розвитку телекомунікаційної сфери в людському суспільстві.

До таких питань, в першу чергу, слід віднести:

- зміст поняття «телекомунікації»;
- значимість телекомунікацій для людини;
- значимість телекомунікацій для суспільства;
- роль телекомунікацій в розв'язанні основних проблем людства (війни, тероризм, голод, зміни клімату, загроза колапсу земної цивілізації).

Інформаційний аналіз цих загальних питань доцільно почати з вироблення загального бачення місця інформації в живій природі. Інформація в природі використовується, перш за все, для побудови органів і тіла окремої особини відповідно до набутих попередніми поколіннями видових ознак (генетична інформація), для оперативного реагування на мінливі умови життя особини (рефлекторна інформація), для отримання прижиттєвого досвіду і оптимізації поведінки особини (навчальна інформація), для узагальнення накопиченої в процесі життя інформації та прогнозування майбутніх умов і дій особини (розумова інформація). З інформаційної точки зору, життя – це безперервні процеси отримання, накопичення, використання, продукування і обміну інформації живими організмами. Без інформації речовина і енергія переходять у рівноважний стан і життя зникає.

Саме в цій інформаційній царині життя особливе місце займають процеси передавання і обміну інформацією, які у загальній формі означаються терміном «комунікації». В україномовній Вікіпедії комунікацій визначено як *«процес обміну інформацією (фактами, ідеями, поглядами, емоціями тощо) між двома або більше особами, спілкування за допомогою вербальних і невербальних засобів із метою передавання та одержання інформації»*.

Найбільш розвинуті комунікації у таких тварин, які процесі еволюції набули досконалу нервову систему з центральним (головним) мозком. Обмін інформацією дозволяє їм координувати поведінку особин у групах, вести колективний (стадний, зграйний) спосіб життя, вести обмін навчальною інформацією і все це – з метою покращення умов життя і збільшення шансів на успіх виживання в конкурентному середовищі проживання.

Здавалося б, що зміст двокореневого терміну «телекомунікації» мав би означати просто «комунікації на далекій відстані». Однак, сьогодні в усьому світі під телекомунікаціями розуміють дещо інше: *«– це передавання, випромінювання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних або інших електромагнітних системах»*. Це визначення наведено в Законі України «Про телекомунікації» і є дослівним перекладом визначення терміну «telecommunications» із словника Міжнародного Телекомунікаційного союзу (ITU) – одного з органів ООН. Офіційне визначення дуже невіддале за кількома аспектами:

1) в ньому не відображено основний зміст процесу телекомунікацій – передавання та обмін інформації на великих відстанях; 2) слово «випромінювання» ставить вдумливого читача у сенсовий ступор – як можна «випромінювати» знаки, письмовий текст, зображення та повідомлення? 3) чому телекомунікації обмежені тільки електромагнітними системами? А поштове пересилання інформації, підводний гідролокаційний зв'язок, світловий або оптичний телеграф – це не телекомунікації? 4) таке визначення вимагає визнати «телекомунікаціями» і електромагнітне передавання (близький радіозв'язок) в карткових, смартфонних і домофонних системах, що семантично дисонує з першою частиною терміну.

Така недбалість у офіційному визначенні терміну «телекомунікації» не просто семантична помилка, а свідчення відсутності у авторів цього визначення загальних (філософських) уявлень про сутність і роль телекомунікацій у живій природі і в людському суспільстві, зокрема. Крім того, вона свідчить про не суттєвість запропонованого визначення терміну «телекомунікації» як для вітчизняного закону «Про телекомунікації», так і для комплексу документів ІТУ. Відсутність такого визначення в зазначених документах не змінює їх сутності, яка, попри досить складні технічні і технологічні деталі, має досить прозаїчний загальний сенс – вони обстоюють комерційні інтереси великої телеком-індустрії під назвою «телекомунікації».

Фактична сутність того, що сьогодні ховається за терміном «телекомунікації» – це транснаціональний синдикат розробників і виробників телекомунікаційно-комп'ютерного обладнання, розробників і торговців програмного забезпечення (застосунків), операторів телекомунікаційних систем, мас-медіа та рекламних агенцій. Основною метою телеком-індустрії є отримання доходів і приватних прибутків у процесі надання споживачам інформаційних і інформаційно-супроводжуваних послуг у дистанційному режимі – телефон, текстовий зв'язок (СМС, чат, телеграми тощо), передавання файлів і даних, доступ до сховищ інформації і знань, електронна торгівля тощо. Такий синдикат більш точно характеризує термін «телекомерція».

Для телекомерції основний сенс телекомунікацій в людському суспільстві відходить на задній план, поступаючись місцем звичайній комерційній діяльності в системі координат ліберально-капіталістичних суспільних відносин. Це дуже невтішний результат прогресу інформаційно-комунікаційних технологій людства, оскільки він не стимулює, а гальмує розвиток земної цивілізації.

Дійсно, інформаційна сфера суспільства – це одна з трьох основ людського буття і існування цивілізації. Обмін інформацією в цій сфері (комунікації) супроводжує усі процеси життєдіяльності суспільства. Без комунікацій неможливі такі ключові процеси як соціалізація дітей у суспільстві, накопичення в суспільній пам'яті і корисних інформаційних внесків від усіх членів суспільства та масове їх використання усіма членами суспільства. Варто відмітити, що процес накопичення і використання інформації людством через механізм суспільної пам'яті (за активної участі телекомунікацій) сприяв експоненційному розвитку земної цивілізації у останні тисячоліття (а особливо у останні 300 років) при незмінності біологічних характеристик людини та її довкілля.

Комерціалізація інформаційної сфери суспільства і сфери телекомунікацій, зокрема, гальмує прогрес людства за чотирма напрямками:

1) вона встановлює цінові бар'єри на шляхах обміну інформацією, що створює інформаційні (цифрові) розриви як всередині суспільства, так і між суспільствами з різним рівнем розвитку; 2) вона відволікає матеріальні ресурси на безупинну гонку телекомерційних засобів, які внаслідок цього мають короткий термін використання і помітно ускладнюють економічні і екологічні проблеми людства; 3) вона зміцнює підвалини ліберально-капіталістичного устрою суспільства, який, це вже очевидно, веде людство до еколого-економічного колапсу; 4) вона не сприяє переходу людства на шлях сталого розвитку.

Принципи комерціалізації телекомунікацій протирічать основним положенням інформаційної філософії [1], згідно з якими інформація є нематеріальною основою життя і вона має вільно циркулювати в живому світі. Людство, маючи обмеження на обсяги речовини і енергії, має майже необмежені можливості розвиватися у інформаційному відношенні. Шлях до такого розвитку відкриває заміна ліберально-капіталістичної парадигми розвитку людства на парадигму сталого розвитку. Попри недостатню сьогоднішню конкретизацію цієї парадигми і відсутність практичного досвіду її реалізації, загальні принципи сталого розвитку людства виглядають доволі очевидними.

Перш за все, людство рішенням ООН повинно узяти на себе відповідальність за напрям і характеристики розвитку земного життя на віддалену перспективу (тисячі років), як це і передбачав Володимир Вернадський у своїх міркуваннях про ноосферу. Така відповідальність вимагає здійснення низки практичних кроків як на світовому (міжнародному) рівні, так і на рівні окремих суспільств (країн), а саме:

- має бути створена потужна наукова платформа для всеосяжного і детального спостереження за станом розвитку земної ноосфери та за усіма основними процесами, що супроводжують цей процес;

- має бути створено всесвітній науковий центр дослідження і прогнозування ноосфери (ЦДПН), який на основі інформації про стан і процеси змін у ноосфері розробляє і постійно актуалізує модель довгострокової еволюції життя на землі, досліджує різні сценарії розвитку ноосфери, розробляє рекомендації для прийняття поточних політичних рішень з такого розвитку;

- на основі прогнозів і рекомендацій ЦДПН, ООН розробляє світову політику практичних дій з розвитку ноосфери, яка містить кількісні і якісні орієнтири для практичних дій кожного із суспільств, у тому числі квоти на споживання основних видів земних ресурсів, на викиди продуктів життєдіяльності та на чисельність населення суспільства;

- політики кожного суспільства деталізують загальні директиви ООН з урахуванням конкретних історичних і культурних особливостей суспільства і забезпечують проведення суспільної політики розвитку тієї частини ноосфери, яка є базою існування і розвитку конкретного суспільства; деталізація директив ООН в даному суспільстві має доводитися і контролюватися до рівня кожної групи і кожного індивіда суспільства;

- інформація про хід і результати реалізації політики розвитку ноосфери конкретного суспільства надсилаються в ООН для узагальнення і коригування світової політики та для ретрансляції їх в ЦДПН, де вона враховуватиметься у наступних циклах прогнозування і вироблення рекомендацій з розвитку земної ноосфери.

Одним із фундаментальних питань переходу людства до парадигми сталого розвитку та її довготривалого дотримання є кардинальна зміна морально-етичних основ кожного суспільства і кожної людини у бік їх екологізації та гуманізму. Питання дуже важке, оскільки морально-етичні основи людства мають властивість передаватися природним шляхом з покоління в покоління майже у незмінному вигляді, подібно до генетичної інформації, і тому в них сьогодні містяться елементи моралі навіть доісторичної людини. Сучасна мораль людства допускає такі прояви антигуманності, як агресія, тероризм, війни, панування-підкорення, розкішність-бідність, необмеженість бажань, не контрольованість дітонародження тощо. Анти-екологічні елементи сучасної моралі допускають неконтрольоване витрачання земних ресурсів, їх перевитрати на демонстративне споживання, невідновлювальне нищення рослинності і фауни біосфери тощо. Проблему зміни моралі людства майже неможливо розв'язати природним шляхом, але цілком можливо політичним шляхом протягом лише одного покоління, якщо узяти до

уваги суто інформаційну сутність моралі і створивши інформаційні умови для зміни моралі.

Дійсно, поведінка людини визначається тією інформацією в її довготривалій пам'яті, яку людина накопичує, в основному, у період соціалізації, а потім доповнює протягом усього життя. Новонароджена людина має пусту довготривалу пам'ять і тому, створивши у суспільстві відповідне інформаційне оточення для новонароджених, можна здійснити досить швидко (за 15-20 років) зміну морально етичних основ цього суспільства. Очевидно, що саме таким шляхом Китай наразі здійснює натурний експеримент з асиміляції у китайське суспільство уйгурів, які мають особливу (мусульманську) морально-етичну основу. В Китаї дорослих уйгурів направляють у спеціальні табори перевиховання, а їх дітей – у спеціальні дитячі інтернати. Очевидно, що без дорослих діти швидше і міцніше засвоюють нові моральні основи життя, а батьки шляхом навчання також можуть поступово забути про свої старі моральні основи і призвичаїться до морально-етичних основ усього Китаю.

Наведені вище основні принципи переходу людства на шлях сталого розвитку передбачають істотне розширення функцій інформаційної сфери в людському житті та відповідної перебудови принципів організації і розвитку телекомунікацій. Роль телекомунікацій незамінна і в процесі зазначеного переходу, і в підтриманні процесів сталого розвитку людства у майбутній ноосфері, за яку воно буде відповідальним протягом необмеженого майбутнього. Природно що в інформаційній сфері людства, орієнтованій на сталий розвиток, роль телекомунікацій істотно розшириться, разом із сферами комп'ютерної індустрії та мас-медіа.

Без телекомунікацій не обійдуться ні процеси соціалізації нових поколінь землян, ні процеси ефективного спостереження за ноосферою, ні процеси контролю за витрачанням земних ресурсів та викидів у ноосферу, ні ефективна, гуманно- і екологоорієнтована виробнича діяльність, ні інтелектуальне і розвивальне дозвілля, ні масштабна космічна діяльність. Однак телекомунікації мають позбутися сьогодишніх ліберально-капіталістичних атавізмів у принципах свого розвитку і функціонування – гонитвою за прибутком і марнотратством земних ресурсів на безконечні версії та релізи все нових телекомунікаційно-комп'ютерних засобів, нехтування процесами оптимізації телекомунікацій під насущні потреби суспільства і кожної людини.

Висновок. Інформаційно-філософський підхід до аналізу і визначення загальних принципів функціонування і розвитку сфери телекомунікацій в людському суспільстві дає можливість розкрити природне значення цієї сфери для функціонування і розвитку людства та досягти оптимальності сфери телекомунікацій в умовах майбутніх суспільств сталого розвитку з мінімальним витрачанням земних ресурсів.

Література

1. Bob Doyle. Great problems in philosophy and physics solved?//First edition/ Cambridge, MA, USA : I-Phi Press,2016. <https://www.informationphilosopher.com/books/>
2. Френк Уебстер. Теории информационного общества//Аспект пресс, М, 2004.
3. ГРЕБЕННИКОВ, Валерій Олександрович. ПРО ДОЦІЛЬНІСТЬ РОЗШИРЕННЯ ПОНЯТТЯ ІНФОРМАТИЗАЦІЇ. Збірник матеріалів Міжнародної науково-технічної конференції «ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ», [S.l.], 2020. ISSN 2664-3057 online. Доступно за адресою: < <http://conferenc.its.kpi.ua/2020/paper/view/20008>>.

ГЕОСТАЦІОНАРНА СУПУТНИКОВА ІНФРАСТРУКТУРА ІНТЕРНЕТУ РЕЧЕЙ

¹Нарушкевич О.М., ¹Жабчик А.І., ²Капштик С.В., ¹Наритник Т.М.

¹*Інститут телекомунікаційних систем КІІ ім. Ігоря Сікорського, Україна*

²*Національний центр управління та випробувань космічних засобів, Україна*

E-mail: sashanarushkevych@gmail.com; nastia2767@gmail.com;

s.kapshtyk@spacecenter.gov.ua; director@mitris.com

THE INTERNET OF THINGS GEOSTATIONARY SATELLITE INFRASTRUCTURE

There is presented the Hierarchical Model of the Internet of Things System that uses a Geostationary Satellite Communication System as a telecommunications infrastructure. Approaches to the introduction of Edge and Fog computing into the Geostationary Satellite Communication Infrastructure to increase the efficiency of the Internet of Things are shown. It is proposed to implement Edge computing at the level of the end user's VSAT Terminal by the Terminal would be equipped with a Computing Module. To implement Fog Computing, it is proposed to equip the Satellite Payload with a separate Computing Module. Peculiarities of Internet information processing in Geostationary Satellite Digital Payload of Transparent and Regenerative type are considered. To increase the efficiency and reliability of the implementation of the Cloud Computing Level, it is proposed to create an Orbital Cloud Network of Data Storage on the basis of Geostationary Satellites - the Cloud Data Centers.

Інтернет речей став важливою складовою частиною сучасних інформаційних технологій [1]. Поширення систем Інтернету речей стримується станом наземної інфраструктури зв'язку, адаптованої до передачі трафіку Інтернету речей. Розширити область надання послуг Інтернету речей дозволяють системи супутникового зв'язку [2]. Існуючі системи супутникового зв'язку застосовуються в системах, що побудовані на хмарній архітектурі. Підвищити ефективність Інтернету речей дозволяє впровадження туманних та граничних обчислень (в іншій літературі – краєвих обчислень) [3]. Завданням досліджень є розробка пропозицій щодо впровадження в геостационарні супутникові системи туманних та граничних обчислень та формування космічної інфраструктури хмарних обчислень.

Туманні та граничні обчислення - це концепція розподілених обчислень, коли частина обчислень, пов'язаних із обробкою та узагальненням інформації Інтернету речей, здійснюється на проміжних рівнях ієрархічної структури Інтернету речей: граничні обчислення – якомога ближче до границі телекомунікаційної мережі, туманні обчислення – на проміжних рівнях передачі інформації. Згідно з цією концепцією після обробки інформації сенсорів Інтернету речей на проміжних рівнях до актуаторів Інтернету речей передаються команди управління, а на рівень хмарних обчислень передається узагальнена інформація про результати обробки та видані команди.

На рис.1 наведено ієрархічну модель геостационарної супутникової системи Інтернету речей. В моделі реалізовано граничні обчислення на рівні VSAT-терміналу через доповнення терміналу обчислювальним модулем, та туманні обчислення на рівні геостационарного супутника великої пропускної здатності через доповнення корисного навантаження супутника додатковим обчислювальним модулем. Геостационарний супутник великої пропускної здатності передає узагальнену інформацію Інтернету речей до станції спряження, яка транслює інформацію до наземних центрів хмарних обчислень, або по лінії зв'язку між супутниками до геостационарного супутника – центру хмарних обчислень космічного базування.

Перспективним напрямком розвитку геостационарних супутників великої пропускної здатності є впровадження цифрового корисного навантаження прозорого або

регенеративного типу [4].

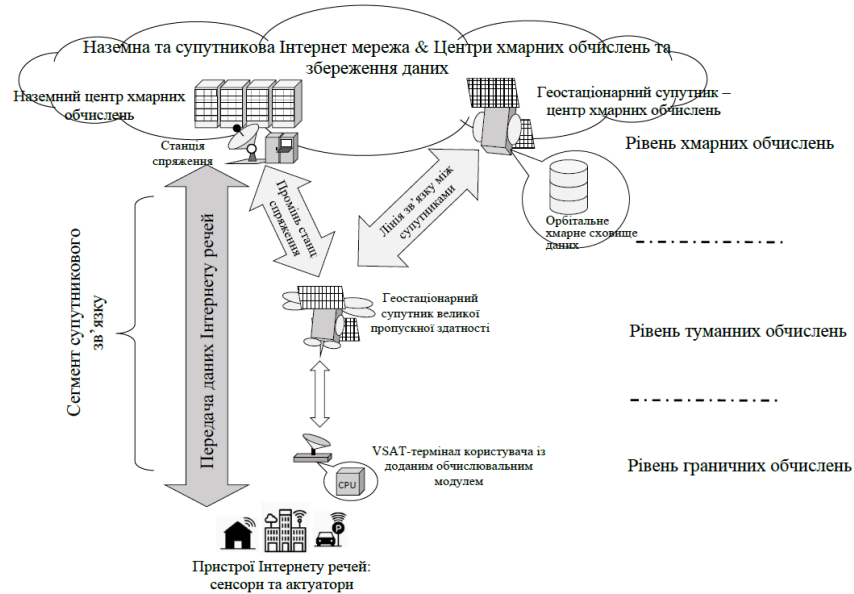


Рис.1. Ієрархічна модель геостационарної супутникової системи Інтернету речей.

Використання технологій цифрової обробки сигналів надає можливість гнучкої дистанційно керованої реконфігурації корисного навантаження без зміни електричних з'єднань. Додатковою перевагою цифрового корисного навантаження для впровадження туманних обчислень Інтернету речей є можливість доповнення корисного навантаження окремим обчислювальним модулем, який призначений для реалізації туманних обчислень. На мал.2 наведено структурну схему цифрового корисного навантаження прозорого типу з додатковим обчислювальним модулем, а на мал.3 наведено структурну схему цифрового корисного навантаження регенеративного типу з обчислювальним модулем.

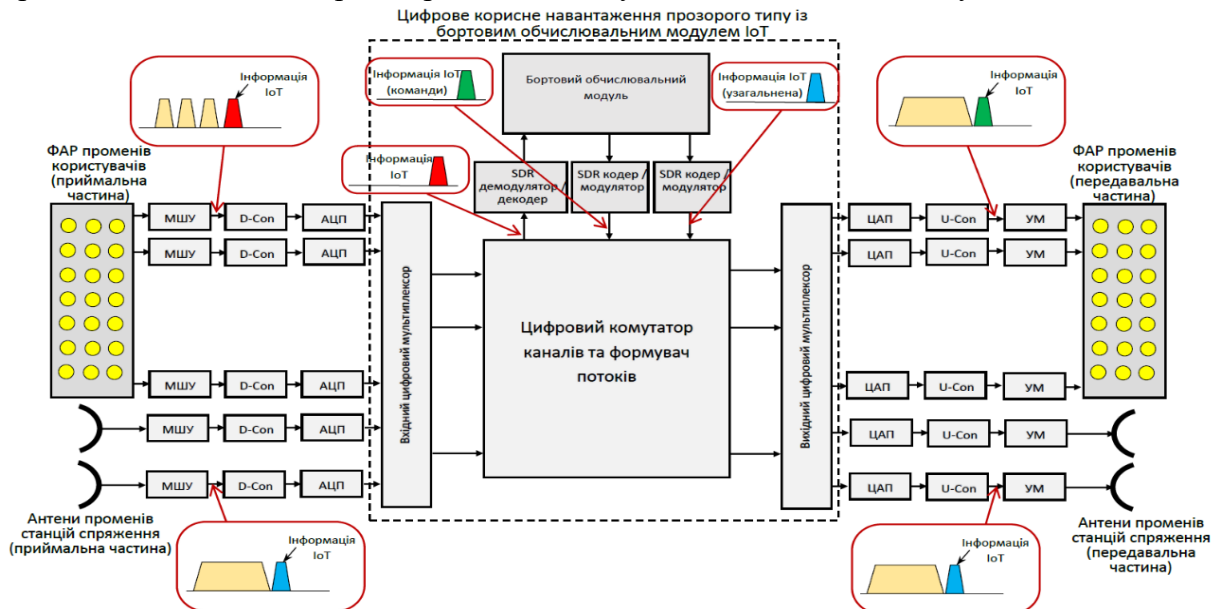


Рис.2. Цифрове корисне навантаження прозорого типу з обчислювальним модулем туманних обчислень.

Цифрове корисне навантаження прозорого типу здійснює в цифровому комутаторі комутацію окремих смуг частот, які виділяються із смуги частот кожного променя (користувачів та станцій спряження). Промені користувачів формуються за допомогою бортової фазованої антенної решітки (ФАР) (див.рис.2).

Смуга частот кожного променя користувачів підсилюється підсилювачем з низьким рівнем шуму (МШУ), переноситься на проміжну частоту в діапазоні L за допомогою конвертора (D-Con) та переводиться в цифровий формат I/Q в аналого-цифровому перетворювачі (АЦП).

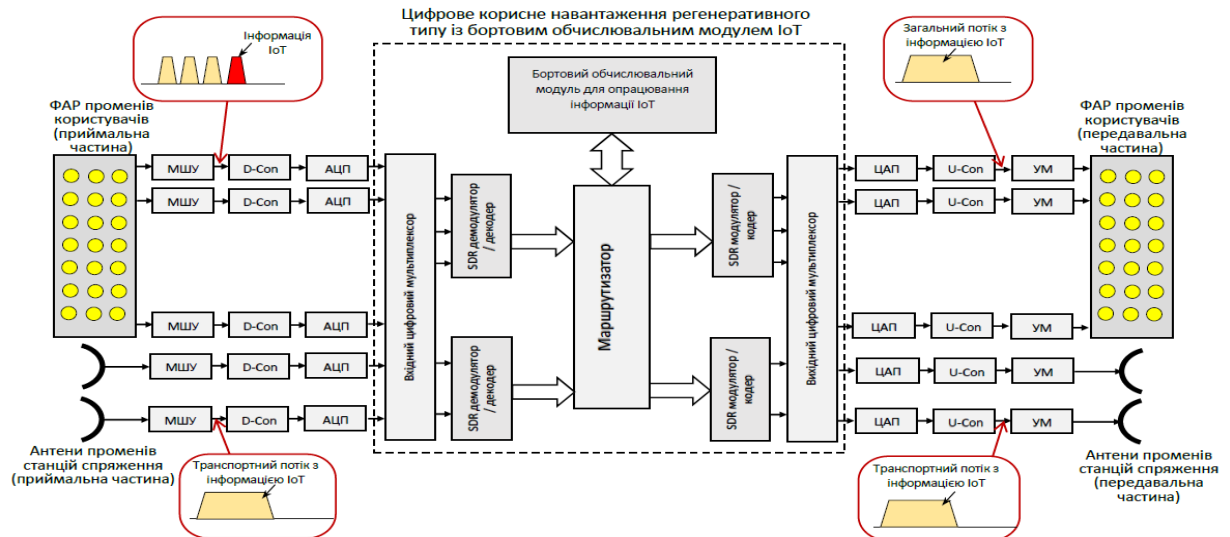


Рис.3. Цифрове корисна навантаження регенеративного типу з обчислювальним модулем туманних обчислень.

Для передачі інформації Інтернету речей в кожному промені користувачів виділяється окрема смуга частот (на рис.2 виділена червоним кольором). Цифровий комутатор комутує ці смуги частот з кожного променя користувачів до демодулятора/декодера, який підключений до бортового обчислювального модуля. Після проведення необхідних обчислень команди управління передаються на кодер/модулятор, з виходу якого інформація передається в окремій смузі частот променю користувачів до актуаторів (на рис.2 виділена зеленим кольором), а узагальнена інформація комутується в окремій смузі частот до променя до станції спряження (на рис.2 виділена синім кольором). Цифровий потік для променів користувачів та станцій спряження поступає на цифро-аналоговий перетворювач, переводиться в аналоговому вигляді до робочого діапазону частот, підсилюється і передається до передавальної ФАР та антени променю станції спряження.

В супутнику із цифровим корисним навантаженням регенеративного типу (рис.3) інформація Інтернету речей поступає по променю користувачів в окремій смузі частот, або в загальному потоці, який формує VSAT-термінал користувача. Смуга частот променю користувачів після підсилення переноситься в діапазон проміжної частоти L та переводиться в цифровий I/Q формат. В корисному навантаженні в цифрових демодуляторах/декодерах проводиться обробка інформації і її подальша маршрутизація здійснюється в маршрутизаторі за змістом адресної частини кожного пакету/блоку. Інформація Інтернету речей направляється до бортового обчислювального модуля для обробки та узагальнення. Інформація управління та узагальнена інформація передаються окремими потоками для включення до загального потоку / мультиплексу лінії до низу променю користувачів та до потоку лінії до низу променю станції спряження.

Сучасні технології виготовлення геостационарних супутників і досвід експлуатації орбітальних угруповань дозволяє вивчати питання про створення орбітального хмарного сховища даних, що складається з декількох геостационарних супутників – хмарних центрів обробки даних (див. рис.4).

Орбітальне хмарне сховище даних є доповненням до наземної хмарної інфраструктури і орієнтоване в першу чергу на обробку і зберігання даних супутникових систем Інтернету речей. Для підвищення надійності зберігання даних і збільшення при необхідності обчислювальної потужності орбітальне хмарне сховище даних взаємодіє з наземною інфраструктурою хмарних центрів за допомогою спеціально виділених радіоканалів – ліній передачі даних до наземної інфраструктури.

Геостационарні супутники високої пропускної здатності забезпечуватимуть доступ до геостационарних супутників-хмарних центрів обробки даних за допомогою ліній зв'язку між супутниками, які працюють в радіочастотному або оптичному діапазоні.

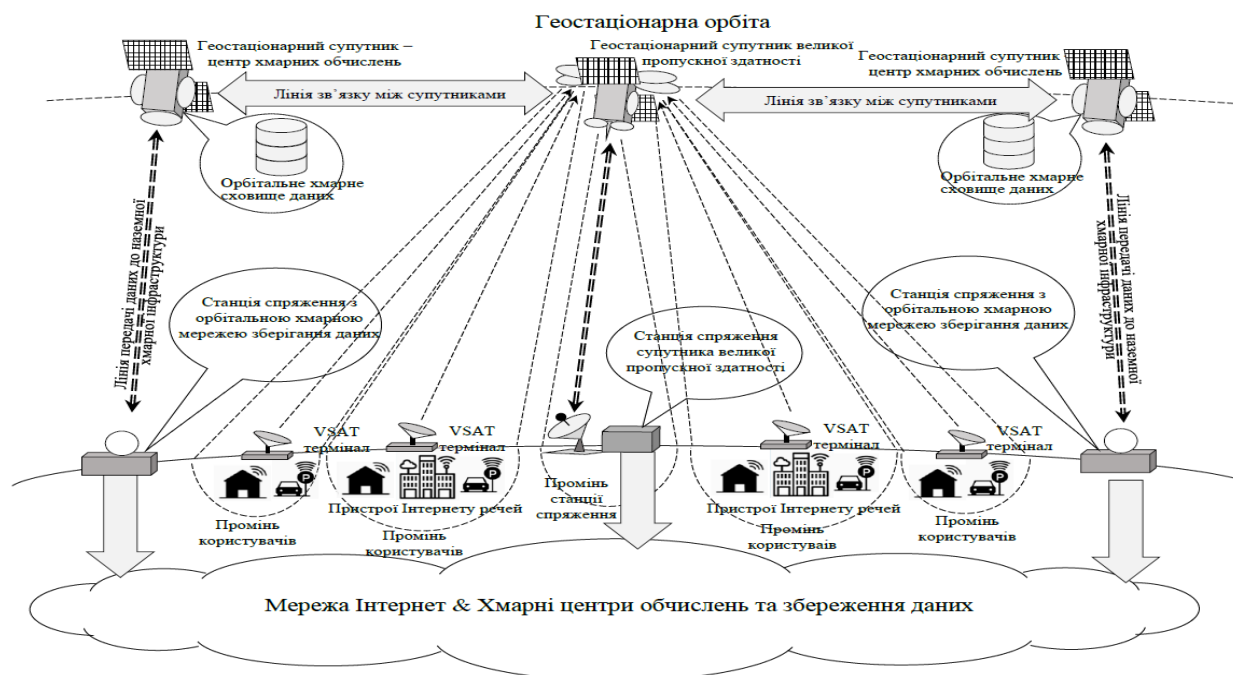


Рис.4. Орбітальна хмарна мережа зберігання даних.

Лінії зв'язку між геостационарними супутниками для забезпечення доступу до орбітального хмарного сховища даних можуть бути побудовані при використанні напрацьованих науково-дослідного інституту КПІ ім. Ігоря Сікорського в області терагерцових технологій [5].

Висновки. Застосування геостационарних систем супутникового зв'язку дозволяє розширити зону надання послуг Інтернету речей незалежно від стану розвитку інфраструктури наземних систем зв'язку та передачі даних.

Впровадження концепції граничних та туманних обчислень в сучасних геостационарних системах із супутниками великої пропускної здатності, що обладнані цифровим корисним навантаженням прозорого та регенеративного типу, можливе через доповнення VSAT-терміналів користувачів та корисного навантаження супутників окремими обчислювальними модулями.

Підвищити надійність та оперативність зберігання та обробки інформації систем Інтернету речей, що використовують геостационарні супутники великої пропускної здатності, на рівні хмарних обчислень можливо шляхом створення на геостационарній орбіті орбітального хмарного сховища даних.

Доступ геостационарних супутників великої пропускної здатності, що реалізують туманні обчислення, до геостационарних супутників – центрів хмарних обчислень може здійснюватися за допомогою ліній зв'язку між супутниками, які використовують терагерцовий діапазон частот.

Література

1. Global IoT market to grow to \$1.5trn annual revenue by 2030/Електронний ресурс. Режим доступу: www.iot-now.com/2020/05/20/102937-global-iot-market-to-grow-to-1-5trn-annual-revenue-by-2030/
2. Gerard Maral, Michel Bousquet. Satellite communications systems - 5th ed. 2009 John Wiley&Sons Ltd.
3. Программируемое управление доступом к сети с адаптивной настройкой физических интерфейсов / А.И. Чернышев, И.О. Демиденко, А.В. Воруев, С.Ю. Михневич / Известия Гомельского государственного университета, № 6 (111), 2018. С.55-62.
4. Overview of Existing and Future Advanced Satellite Systems / John Nguyen / DOI: 10.5772/intechopen.93227 / Електронний документ Режим доступу: <https://www.intechopen.com/online-first/overview-of-existing-and-future-advanced-satellite-systems>.
5. Development of the transmitting and receiving channels for terahertz band relay systems (2015) / Ilchenko, M. Ye., Narytnyk, T.M., Radzikhovsky, B.M., Kuzmin, S.E., Lutchak, O.V. / Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika), 74 (11), pp. 981-998. / Режим доступу: www.dl.begellhouse.com/journals/0632a9d54950b268,7d1efd50245bb694,2d7e62e457ab16bd.html

МЕТОДИ АУТЕНТИФІКАЦІЇ НА ОСНОВІ ПУБЛІЧНОГО КЛЮЧА В СИСТЕМІ ІНТЕРНЕТУ РЕЧЕЙ

Дуля О.О., Міночкін Д.А.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

Email: sasa97973@gmail.com

METHODS OF THE PUBLIC-KEY BASED AUTHENTICATION IN THE INTERNET OF THINGS

This paper considered a comparative analysis of the methods of the public-key based authentication in the Internet of Things, and the optimal solution based on the comparison is given.

В системі Інтернету Речей (Internet of Things, IoT), аутентифікація - це процес ідентифікації користувачів, пристроїв, додатків і обмеження доступу до авторизованих користувачів і некерованих пристроїв або послуг.

Розглянемо аутентифікацію за допомогою відкритого ключа. У цьому процесі використовуються криптографічні схеми, засновані на імені користувача та паролі, щоб забезпечити надійну безпечну операцію над IoT.

До методів аутентифікації за допомогою відкритого ключа відносяться [1]:

- Симетричне шифрування.
- Шифрування за допомогою публічного ключа, або асиметричне шифрування (Public-key cryptography, PKC).
- Інфраструктура відкритих ключів (Public-key infrastructure, PKI).

Симетричне шифрування використовується для забезпечення конфіденційності повідомлення при його передачі, зберіганні та обробці. Алгоритм симетричного ключа виконує операції шифрування / дешифрування на основі одного ключа, яким користуються дві або більше сторін. Трудність в симетричній криптографії полягає в безпечній доставці ключа від кодувальника до декодера, що може створити ризик безпеки. Той, хто отримує доступ до симетричного ключа, може отримати доступ / змінити / надіслати повідомлення без відома одержувача, що повідомлення було змінено. Для вирішення цих проблем було розроблене шифрування відкритим ключем.

Алгоритми симетричних ключів досить ефективні, але передача ключів є досить складною для кінцевих пристроїв IoT. Розподіл ключів вимагає надійного зв'язку між сервером розподілу ключів та вузлами IoT. РКС ефективним способом забезпечення конфіденційності та аутентифікації. На відміну від симетричного шифрування, РКС базується на математично складній для вирішення задачі [2]. Шифрування відкритим ключем базується на функціях, які легко обчислити, але важко повернути назад без додаткової інформації. У криптосистемі РКС, як правило, у парі ключів, відкритому та приватному ключах, відкритий ключ стає доступним для клієнта, а приватний ключ зберігається в безпечному місці. Захищеність системи безпеки РКС полягає в тому, наскільки важко визначити правильно створений приватний ключ за його відкритим ключем. У цьому випадку довжина закритого ключа важлива для уникнення брут-форс (метод підбору) атак.

RSA (аббревіатура від прізвищ Rivest, Shamir та Adleman) - це широко використовуваний алгоритм в шифруванні за допомогою відкритого ключа, в якому складною для обчислення проблемою є пошук простих множників складеного числа [3]. RSA є однією з перших практичних криптосистем з відкритим ключем, яка базується на практичній складності розкладу на добуток двох великих простих чисел. Якщо відкритий ключ достатньо великий, лише той, хто знає прості числа, може здійснити декодування повідомлення. RSA є відносно повільним алгоритмом шифрування, однак він зазвичай використовується для передачі зашифрованих спільних ключів для симетричного шифрування. Оскільки RSA-шифрування є ресурсоємною операцією, в IoT воно використовується в поєднанні з симетричною криптографією. Спільний симетричний ключ зашифрований RSA; безпека шифрування в цілому залежить від довжини ключа. Для RSA потрібна довжина ключа 1024 біта (128 байт), щоб мати еквівалентний рівень безпеки симетричної криптографії довжиною ключа 128 біт (16 байт) [1]. Великий розмір ключа RSA призведе до великих витрат на обчислення.

Еліптична криптографія (Elliptical curve cryptography, ECC) є альтернативою RSA та має кращий захист від атак методом підбору ключів [3]. ECC краще підходить для IoT завдяки значно меншому бітовому розміру операндів у середовищі, обмеженому ресурсами. ECC - ще один підхід до криптографії з відкритим ключем, який працює на основі еліптичних кривих

над скінченними полями. Щоб мати еквівалентний рівень безпеки симетричної криптографії довжиною ключа 128 біт (16 байт) для ключа з ЕСС шифруванням необхідно 256 біт (32 байт) [1]. Це ефективніше, ніж RSA, і більше підходить для пристроїв з обмеженими ресурсами в Інтернеті речей.

Проблемою використання криптографії з відкритим ключем є впевненість/доказ того, що певний відкритий ключ є справжнім. Він правильний і належить заявленій фізичній або юридичній особі, і не був змінений або замінений зловмисником або третьою стороною. Звичайний підхід до вирішення проблеми полягає в використанні РКІ, в якому одна або кілька третіх сторін, відомі як центр сертифікації (Certification authority, CA), засвідчують право власності на пари ключів.

РКІ - це набір ролей, політик та процедур, необхідних для створення управління, розповсюдження, використання, зберігання та скасування цифрових сертифікатів та управління шифруванням із відкритим ключем. В середовищі IoT загальною проблемою відкритого ключа є вимога аутентифікованого обміну відкритими ключами. РКІ складається з компонентів для надійного розповсюдження відкритих ключів. Найважливішим в РКІ є довірена третя сторона, яка підписує ідентифікатор сутності своїм приватним ключем.

Висновки. Для системи Інтернету Речей найкращим є метод аутентифікації на основі інфраструктури відкритих ключів (РКІ), з використанням ЕСС шифрування для передачі симетричних ключів.

Література

1. Mousavi, S.K., Ghaffari, A., Besharat, S. et al. Security of internet of things based on cryptographic algorithms: a survey. *Wireless Netw* 27, 1515–1555 (2021).
2. Mousavi, S.K., Ghaffari, A., Besharat, S. et al. Improving the security of internet of things using cryptographic algorithms: a case of smart irrigation systems. *J Ambient Intell Human Comput* 12, 2033–2051 (2021).
3. Shancang Li, Li Da Xu *Securing the Internet of Things* // Syngress, 2007, pp 69-95.

ВИКОРИСТАННЯ ЦИФРОВИХ АНТЕННИХ РЕШТОК ДЛЯ ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ ПРИЙОМУ СИГНАЛІВ НАВІГАЦІЙНОЇ СИСТЕМИ GPS

¹Вигівський М.С., ¹Денисенко М.С., ²Капштик С.В., ¹Наритник Т.М.

¹Інститут телекомунікаційних систем, КПІ ім. Ігоря Сікорського, Україна

²Національний центр управління та випробувань космічних засобів, Україна

E-mail: huaweibgablek@gmail.com; maxdeniss56@gmail.com;

s.kapshtyk@spacecenter.gov.ua; director@mitris.com

UTILISATION OF DIGITAL BEAMFORMING TO INCREASE INTERFERENCE PROOF OF GPS NAVIGATION SYSTEMS SIGNAL RECEPTION

The method of simulation (spoofing) interferences formation of reception of GPS radio navigation system signals is investigated. It is shown that the using of additional information from space monitoring systems NORAD can improve the solution of the problem of detecting the source of radiation spoofing noise. It is proposed to use a digital beamforming technology to measure the directions of reception of GPS satellite signals and spoofing interference. A method and a block diagram of a device for determining the structure of a spoofing noise have been developed.

У період швидкого технічного розвитку інформаційних та телекомунікаційних технологій та побудованих на їх основі систем та засобів Інтернету речей зростає важливість супутникових радіонавігаційних систем, таких, як GPS NAVSAR, GNSS та інших [1]. Але розвиток цих систем супроводжується розвитком методів та засобів, які спрямовані та ускладнення використання супутникових радіонавігаційних систем, створення радіозавад та спотворення сформованого навігаційного поля. Одним із методів спотворення радіонавігаційного поля є застосування імітаційних, або спуфінгових завад. Ці завади формуються шляхом перевипромінювання одного або декількох сигналів радіонавігаційних супутників з іншого місця та з певною затримкою. В результаті, виникає зсув радіонавігаційного поля в районі застосування спуфінгової радіозавади, що спричиняє труднощі у визначенні поточного положення рухомих об'єктів та визначення їх поточних навігаційних параметрів (ПНП).

Вирішити проблему протидії негативному впливу спуфінгових завад можливо шляхом комплексного використання інформації від супутникової радіонавігаційної системи та від системи контролю космічного простору, системи NORAD. При формуванні спуфінгової завади вважається, що GPS приймач користувача та контрольно-корегувальні станції (ККС) обладнані неспрямованими приймальними антенами, які не забезпечують просторову селекцію прийнятих сигналів. Але в разі застосування просторової селекції напрямків прийому сигналів GPS на підставі інформації NORAD, яка поступає у вигляді дволінійних елементів TLE (англ. скорочення Two-Line Element) можливо виявити напрямки прийому спуфінгової завади та визначити структури сигналів GPS, що не використовуються в якості зразка для спуфінгової завади. Ці неспотворені сигнали будуть вважатись перевіреними сигналами, або сигналами з високим рівнем довіри. На підставі такого аналізу до користувачів радіонавігаційної системи можна довести каталог супутників, сигнали яких мають високий рівень довіри і по сигналах яких можна розраховувати ПНП.

Метод визначення сигналів GPS з високим рівнем довіри функціонує наступним чином. На рис.1 наведено ситуаційну схему системи GPS. На малюнку позначено точку розташування контрольної станції і показано площину місцевого горизонту. В площині

місцевого горизонту показано напрямок на північ, та вектори напрямків на супутники GPS, що спостерігаються у видимій частині небесної сфери. Для кожного супутника, що спостерігається, визначено вектор напрямку, який описується кутами азимуту та місця $(\alpha, \beta)_{P,s}$. Нижній індекс P,s визначає номер орбітальної площини P та номер супутника в цій площині s . Орбітальне угруповання системи GPS сформоване таким чином, що постійно в полі зору спостерігача на поверхні Землі знаходиться 8-12 супутників (із врахуванням додаткових супутників в кожній орбітальній площині).

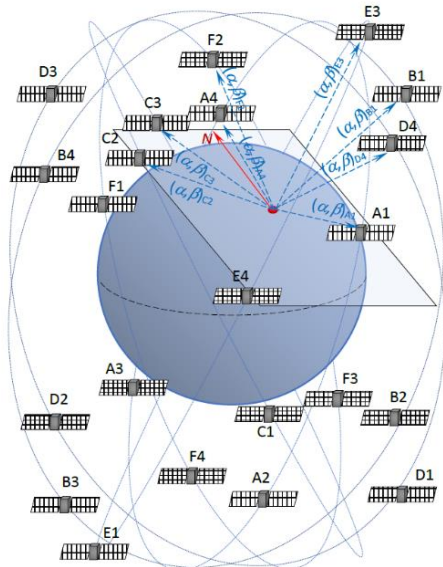


Рис.1. Ситуаційна схема супутникової радіонавігаційної системи GPS.

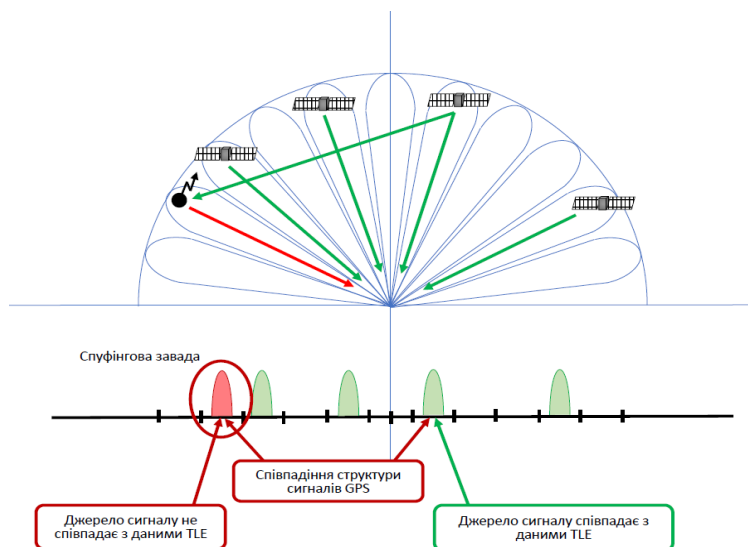
Система NORAD надає інформацію у форматі TLE, яка дозволяє отримати вихідну інформацію для розрахунку ПНП кожного супутника GPS. Пакет даних TLE містить інформацію (див. табл. 1).

Математичний апарат для розрахунку ПНП супутників GPS на час проведення вимірювань наведений в [2].

Забезпечити ефективну просторову селекцію сигналів GPS можливо із використанням технології цифрової антенної решітки (ЦАР) [3]. На рис. 2 наведено приклад формування приймальних променів ЦАР в одній площині, які розділяють по напрямках прийом сигналів чотирьох супутників GPS та джерела випромінювання спуфінгової завади.

Таблиця 1. Інформація пакета даних TLE.

Елемент	Позначення
Час епохи (Epoch)	t_0
Нахил (Inclination)	i
Довгота висхідного вузла (R.A. of the Ascending Node)	$a_{\Omega 0}$
Ексцентриситет (Eccentricity)	e
Аргумент перигею (Argument of Perigee)	ω_0
Середня аномалія (Mean Anomaly at Epoch)	M_0
Частота обертання (середній рух, Mean Motion)	n



Комплексний сигнал просторової частоти, яка відповідає азимуту $\alpha_{P,s}$ та куту місця $\beta_{P,s}$ для GPS-супутника номер s , який знаходиться в орбітальній площині P , визначається виразом.

Рис. 2. Формування приймальних променів ЦАР для визначення напрямків прийому сигналів супутників GPS та спуфінгової завади.

$$\dot{Y}_{P,s}(\alpha_{P,s}, \beta_{P,s}) = \sum_{n=-\frac{N}{2}}^{\frac{N}{2}} \sum_{m=-\frac{N}{2}}^{\frac{N}{2}} \dot{W} a_{P,s} \exp[j(nd-1)\alpha_{P,s}] \exp[j(md-1)\beta_{P,s}]$$

де: N – розмірність ЦАР; $\dot{W}$ – ваговий коефіцієнт, який застосовується для поліпшення спрямованості променів ЦАР; $a_{P,s}$ – амплітуда сигналу GPS супутника номер (P,s) в місці розташування ЦАР; d – «крок» ЦАР (відстань між сусідніми елементами, зазвичай $d=\lambda/2$)

Порівняння напрямку прийому сигналу кожного супутника GPS із даними ПНП, які розраховані на підставі інформації TLE, дозволяє виявити джерело випромінювання спуфінгової завади та номер супутника, сигнал якого імітується або перевипромінюється передавачем завади.

На мал.3 наведено структурну схему, що пояснює принцип визначення джерела спуфінгової завади та структури сигналу GPS, який імітується передавачем завади. ЦАР здійснює прийом сигналів GPS від супутників, що знаходяться у видимій частині небосхилу. Сигнали просторових частот, які сформовані ЦАР, поступають до Массиву просторових частот. Кожна просторова частота визначає рівень сигналу, який приймається променем, що спрямований по куту азимуту та куту місця відносно площини місцевого горизонту. Обчислювач поточних навігаційних параметрів супутників GPS на підставі даних TLE обраховує очікувані значення для кутів азимуту та місця для кожного супутника на час проведення вимірювань. Массив даних просторових частот та результати обчислення ПНП супутників GPS надходять до Матриці співпадин просторових частот сигналів GPS з ПНП супутників GPS. В разі співпадин приймається рішення про підтвердження достовірності напрямку прийому сигналу GPS. В разі неспівпадин фіксується факт виявлення напрямку прийому спуфінгової завади.

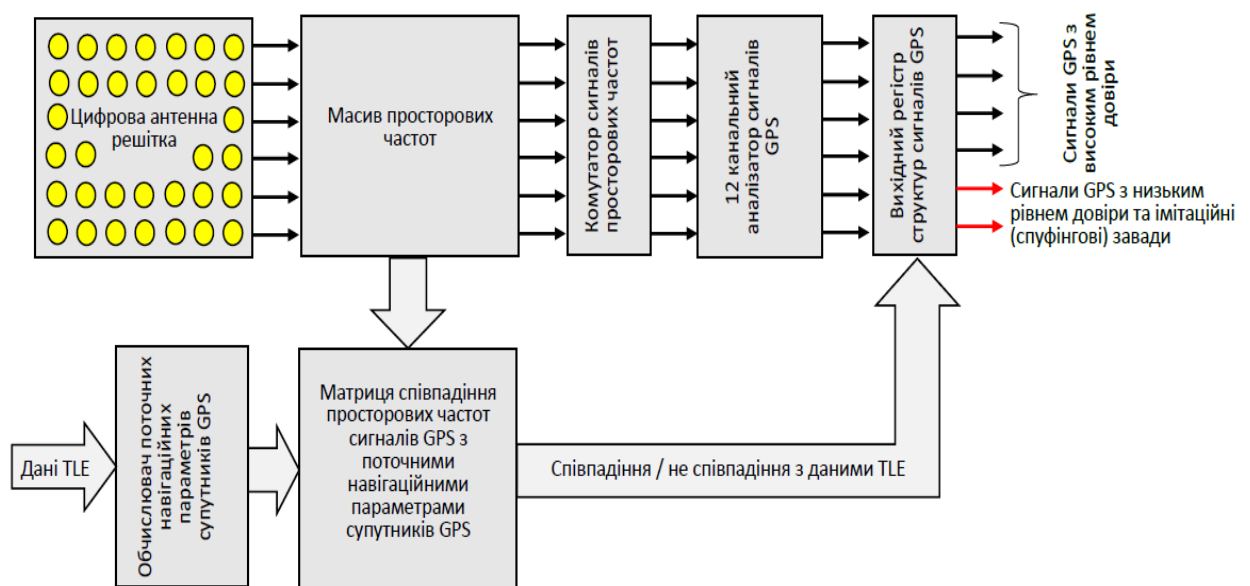


Рис.3. Структура схема вимірювального комплексу.

Для визначення структури спуфінгової завади використовується додаткова лінійка обладнання. Сигнали з виходу Масиву просторових частот через комутатор сигналів просторових частот, який комутує лише сигнали, що перевищили визначений поріг, надходять на 12 каналний аналізатор сигналів GPS. Аналізатор сигналів на підставі аналізу змісту кадру навігаційного повідомлення кожного супутника GPS визначає номер супутника, який передавав виділений сигнал. Результати визначення номерів супутників GPS надходять до вихідного регістру структур сигналів GPS, де здійснюється їх порівняння з метою виявлення повторення. Для прискорення процедури порівняння та виявлення повторення на керуючий вхід вихідного регістру надходить інформація від Матриці співпадіння про виявлені напрямки прийому спуфінгової завади. В результаті обробки на виході Вихідного регістру формується перелік сигналів GPS, які мають високий рівень довіри і які можуть використовуватись споживачами для визначення своїх ПНП, та перелік структур сигналів GPS, що застосовуються в якості спуфінгової завади, і які не доцільно використовувати для розрахунку ПНП користувачами. Така інформація по каналах зв'язку доводиться до кінцевих споживачів.

Висновки. Ефективним методом виявлення джерел випромінення спуфінгових завад є комплексне використання вимірювань просторових координат джерел випромінення сигналів та розрахункових даних щодо поточних навігаційних параметрів супутників радіонавігаційних систем.

Запропоновано технологію вимірювань просторових координат джерел випромінення сигналів супутникових радіонавігаційних систем на базі цифрових антенних решіток.

Комплексе використання результатів вимірювань просторових координат джерел випромінення сигналів супутникових радіонавігаційних систем та даних систем контролю космічного простору дозволяє визначити напрямок на джерело випромінення імітаційної (спуфінгової) завади та визначити структуру сигналу, що перевипромінюється в якості завади. Результатом вимірювань є каталог супутників GPS, сигнали яких мають високий рівень довіри і можуть використовуватись споживачами послуг системи GPS для розрахунку власних поточних навігаційних параметрів.

Література

1. Системы спутниковой радионавигации / Конин В.В., Харченко В.П.; Национальный авиационный университет – К.: Холтех, 2010. – 520 с.
2. Расчет движения космического аппарата по околокруговой орбите по данным TLE по упрощенной модели SGP / Чагина В.А., Гришко Д.А., Майорова В.И. / Наука и образование. МГТУ им. Н.Э. Баумана. Электронн. Журн. 2016 № 01. С 52-66. / DOI: 10.7463/0116.0830533 / Электронный ресурс. Режим доступа: <http://technomag.bmstu.ru/doc/830533.html>
3. Григорьев Л.Н. Цифровое формирование диаграммы направленности в фазированных антенных решетках. – М.: Радиотехника, 2010. – 144 с., ил.

ОГЛЯД СУПУТНИКОВОГО ІНТЕРНЕТУ STARLINK

Нсер А.М., Міночкін Д.А.

Інститут телекомунікаційних систем КПП ім. Ігоря Сікорського, Україна

E-mail: nser.anzhela@gmail.com

STARLINK SATELLITE INTERNET REVIEW

This article will describe the Starlink satellite Internet system. Namely, the construction of this system and the operation of satellites, their location and number. The principle of operation, technology and the current state of the whole project.

В цій статті описано супутниковий інтернет системи Starlink. А саме побудова цієї системи та робота супутників, їх розташування та кількість. Принцип роботи, технології та теперішній стан всього проекту.

Starlink — проект американської компанії SpaceX щодо розробки високопродуктивної супутникової платформи для виготовлення супутників зв'язку та запусків великої їх кількості (сузір'я) у космос. Утворена таким чином нова система зв'язку зможе надавати доступ до широкосмугового (високошвидкісного) Інтернету у віддалених від комунікацій місцях.

Відповідно документам, поданим до Федеральної комісії зі зв'язку США, супутники у космосі спілкуватимуться між собою на частоті понад 10^3 ГГц за допомогою лазерного променя. Із наземними станціями та терміналами користувачів зв'язок здійснюється у радіо (Ku- та Ka-) діапазонах на частоті 12 ГГц. Ku-антени більш надійні у роботі навіть у хмарну та дощову погоду, а Ka-антени забезпечують значно більшу пропускну здатність.

Станом на 11 лютого 2021 року SpaceX запустила 1085 супутників Starlink (включаючи демонстраційні супутники Tintin A і B), а на орбіті знаходяться 1021 супутник. Вони планують запускати до 60 додаткових супутників на рейс Falcon 9, причому запуски будуть проводитися кожні два тижні в 2021 році. В цілому планується розгорнути близько 12 000 супутників з можливим подальшим розширенням до 42 000.

У лютому 2021 року Маск заявив, що супутники рухаються по 25 орбітам, згрупованим між 53 градусами на північ і південь від екватора.

Космічні апарати Starlink спеціально сконструйовані для групового запуску двома стопками по 30 супутників під обтічником ракети Falcon 9 і мають розміри: довжина - 3,2 м, ширина - 1,6 м, висота - 0,2 м.

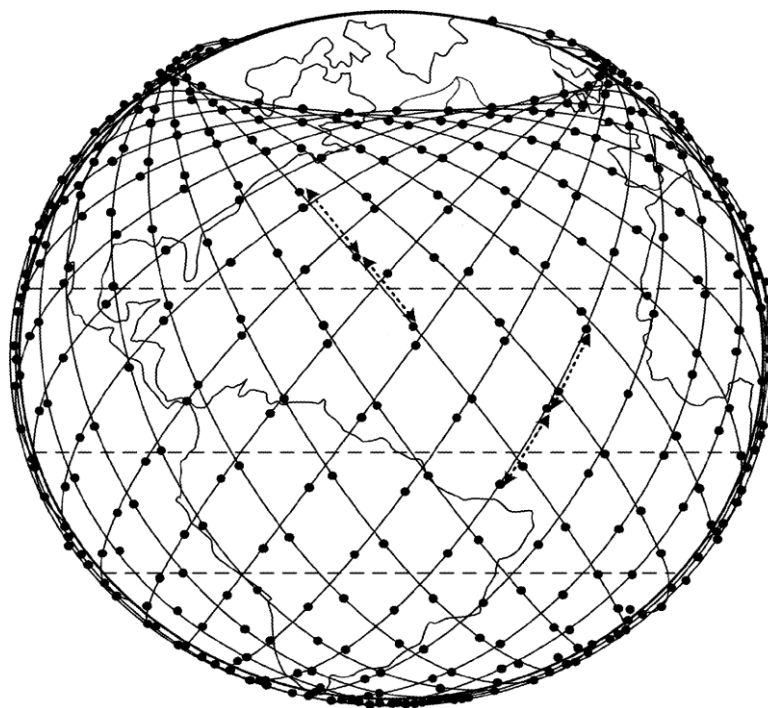


Рис.1. Поточний вигляд угруповання Starlink.

Архітектура мережі Starlink складається з космічного і наземного сегменту. Космічний сегмент - це супутники на низькій орбіті (на даний момент розгортаються перші 1 600 супутників на орбіті заввишки 550 км з нахилом 53 градусів). Наземний сегмент:

- Центр управління мережею (Network Management System),
- Шлюзові станції (Gateway),
- Абонентський термінал (User Terminal).

Після виведення групи супутників на опорну орбіту (як правило це 280 км) супутники розкривають сонячні батареї, встановлюють контакт з наземним Центром управління і проводять перевірку на працездатність і відсутність пошкоджень при відділенні від ракети, далі вони активують електроракетні двигуни (ЕРД) на кріптоні і починають рух на робочу орбіту, яке займає 2-3 місяці. Сонячні батареї при запуску складені "гармошкою" і мають 12 сегментів, де довга сторона кожного сегмента дорівнює ширині супутника. Для переміщення супутника з опорної орбіти 280 км на робочу 550 км і утримання його на ній використовуються плазмові двигуни або електроракетні двигуни.

Електроракетні двигуни мають запас кріптонію орієнтовно 5-10 кг, який заправлений в шаробалони високого тиску. Даний запас дозволить підняти супутник на кругову орбіту 550 км, утримати супутник на ній протягом п'яти років, а потім змінити орбіту з круговою на еліптичну, змінивши перигей з 550 км до, припустимо, 250 км, де за рахунок гальмування об залишки атмосфери супутник досить швидко загальмується і згорить. Основний

корисним навантаженням супутника Starlink є 2 антенних комплексу для зв'язку з шлюзовими станціями і з абонентськими терміналами.

Перебуваючи на орбіті в 550 км, супутник може покрити своїм сигналом пляма на Землі радіусом 950 км (тобто діаметром приблизно 1900 км) за умови, що кут місця для абонентського термінала не буде менше 25 °. Відзначимо, що ефективна робота антен з плоскою фазованою решіткою можлива при куті місця 40 ° і більше.

Діаграма спрямованості антени - дуже важливий параметр антени, і головним критерієм тут є кут, на якому потужність сигналу в 2 рази вище. Чим більше діаметр (площа) антени, тим менше кут діаграми спрямованості і більше її коефіцієнт посилення.

Центр управління мережею забезпечує управління всією мережею супутникового зв'язку, координацію роботи шлюзових і абонентських станцій, завдання єдиного часу в мережі, виділення частотних слотів на супутниках для роботи (передачі даних) шлюзових і абонентських станцій, ведення білінгу, збору даних про передану і отриманої інформації, збір даних про стан системи.

Шлюзові станції забезпечують передачу інформації з мережі інтернет через супутник на абонентські термінали.

Система не буде безпосередньо підключатися зі своїх супутників до мобільних телефонів. Замість цього він буде пов'язаний з плоскими терміналами, які будуть мати фазовані антенні решітки і відслідковувати супутники. Термінали можна встановити де завгодно, якщо вони бачать небо.

Варто зауважити, що на офіційному сайті зазначено, що покриття для України буде в 2022 році. І вже зараз можна здійснити передплату та купити обладнання.

Starlink є найбільшим проектом в області супутникового зв'язку, а можливо, і всієї галузі телекомунікацій в XXI столітті, і дає теоретично шанси на те, що супутниковий зв'язок знову стане актуальний, бо останні 20 років вона поступово поступалася волоконно-оптичних ліній в сегменті магістральних каналів і стільникового зв'язку - на ринку ширококутового доступу в інтернет для кінцевого споживача.

Література

1. Cole, Richard E. (2020). "A Sky Brightness Model for the Starlink "Visorsat" Spacecraft".
2. Енциклопедія Starlink / [Електронний ресурс] - Режим доступу: <https://www.comnews.ru/content/209438/2020-10-07/2020-w41/enciklopediya-starlink#toc5>.
3. Tregloan-Reed, J.; Otarola, A.; Ortiz, E.; Molina, V.; Anais, J.; González, R.; Colque, J. P.; Unda-Sanzana, E. (2020). "First observations and magnitude measurement of Starlink's Darksat".
4. Starlink — Спутниковый интернет от Илона Маска: Разбор/ [Електронний ресурс] - Режим доступу: <https://habr.com/ru/company/droider/blog/528920/>.

АНАЛІЗ ТЕХНІЧНИХ РІШЕНЬ ДЛЯ ПОБУДОВИ МЕРЕЖІ ІОТ НА ПІДПРИЄМСТВІ

Нікішин В. Ю., Міночкін Д.А.
*Інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: vasyi.nikishyn@gmail.com*

ANALYSIS OF TECHNICAL SOLUTIONS FOR BUILDING AN IOT NETWORK AT THE ENTERPRISE

There are a lot of the latest technologies and modern technical solutions in the field of IoT. But many companies in Ukraine and around the world do not use IoT networks. The job is to analyze technical solutions in this area and determine whether it is profitable to install network data in enterprises, and how much the quality of manufacturing will change.

В світі з'являється велика кількість новітніх технологій та сучасних технічних рішень в сфері ІоТ. Але багато підприємств в Україні та світі не використовують ІоТ мережі. Робота полягає в тому щоб проаналізувати технічні рішення в цій сфері та визначити чи вигідно встановлювати дані мережі на підприємствах, та на скільки зміниться якість виготовлення продукції.

З розвитком нових наукових технологій в світі збільшується потреба в автоматизації виробництва та виробничих процесів. Це все призводить до того що людство стоїть на порозі нової промислової революції під назвою «4.0.Індустрія».

Новітні технології стрімко проникли в усі сфери нашого життя та почали змінювати цілі галузі. Саме ця епоха інновацій спричинила нову промислову революцію, де важливу роль відіграє аналіз даних та повна автоматизація виробництва. Найбільш ближчими до цієї революції знаходяться такі країни як: Японія, США, Південна Корея, Німеччина та ін. Для переходу України на нові стандарти у всіх сферах, в особливості промислової сфери, буде супроводжувати ряд проблем.

В багатьох підприємствах у світі, можливо виникнення проблем з переходження на повну автоматизацію через те, що вони працюють на застарілому обладнанні. Даний критерій також впливає на підвищення якості продукції та зниження собівартості. Оперативний збір та аналіз даних стане важким випробуванням для власників бізнесу. Саме це спричинить низку додаткових нових завдань, які неможливо буде вирішити використовуючи старі методи.

В першу чергу, будь-яке промислове підприємство повинно замислитися над технологічною базою, підвищенням продуктивності, зниженням витрат на виробництво, контролем якості продукції, що випускається. Ті, хто не зможе конкурувати в сучасних економічних ринкових реаліях – стануть непотрібними для інноваційної епохи і просто

зникнуть [1].

Для автоматизації великих підприємств використовується індустріальний інтернет речей (Industrial Internet of Things, IIoT) - інтернет речей для корпоративного / галузевого застосування - система об'єднаних комп'ютерних мереж і підключених промислових (виробничих) об'єктів з вбудованими датчиками і ПО для збору та обміну даними, з можливістю віддаленого контролю і управління в автоматизованому режимі, без участі людини.

Принцип роботи технології полягає в наступному: спочатку встановлюються датчики, виконавчі механізми, контролери та людино-машинні інтерфейси на ключові частини обладнання, після чого здійснюється збір інформації, яка згодом дозволяє компанії придбати об'єктивні і точні дані про стан підприємства. Оброблені дані доставляються в усі відділи підприємства, що допомагає налагодити взаємодію між співробітниками різних підрозділів і приймати обґрунтовані рішення.

Крім цього, компанії можуть замінити швидко застаріваючу паперовий документообіг електронним, а також акумулювати експертні знання фахівців

Отримана інформація може бути використана для запобігання позапланових простоїв, поломок устаткування, скорочення позапланового техобслуговування і збоїв в управлінні ланцюгами поставок, тим самим дозволяючи підприємству функціонувати більш ефективно.

Вважається, що IIoT-рішення дозволяють підвищити ефективність виробництва в кілька разів, а термін окупності таких проектів в більшості випадків не перевищує декількох місяців.

Одним із прикладів є завод з виробництва бритв Philips що розташований в Голландії. Обладнання підприємства працює в неосвітленому приміщенні, де встановлені 128 роботів, а весь персонал заводу складається всього з 9 працівників.

Яскравим прикладом застосування Промислового Інтернету Речей є проект компанії Harley Davidson, яка виробляє знамениті мотоцикли. Основною проблемою, з якою зіткнулася компанія, була повільна реакція на запити споживачів в умовах зростаючої конкуренції і обмежена можливість кастомізації дилерами п'яти моделей, що випускаються. У період з 2009 по 2011 рік компанія провела масштабну реконструкцію своїх виробничих майданчиків. В результаті була створена єдина складальна майданчик, що випускає мотоцикли всіх п'яти моделей з можливістю їх кастомізації, при цьому замовнику пропонується вибір з понад 1300 варіантів.

В ході всього виробничого процесу використовуються датчики, керовані системою класу MES. Кожен верстат, кожна деталь має радіопозначку, яка однозначно ідентифікує виріб і його виробничий цикл. Дані від датчиків передаються в платформу обробки даних, що виконує роль інтеграційної шини для збору даних з датчиків і різних інформаційних систем, як внутрішніх виробничих і бізнес-систем компанії Harley Davidson,

так і інформаційних систем контрагентів компанії [3].

В Україні приклад автоматизованого підприємства є Метрологічний центр Регіональної газової компанії. Наразі це єдине у Східній Європі метрологічне підприємство, яке працює як Smart Factory: автоматизоване обладнання кращих світових виробників забезпечує виконання повного технологічного циклу повірки лічильника в повністю автоматизованому режимі, без участі людини. Потужності Центру дозволяють проводити комплексний сервіс 200 тис побутових лічильників газу в рік.

РГК Метрологічний центр у Харкові не має аналогів не лише в Україні, але й у країнах Східної Європи – він був побудований з нуля за принципами Industry 4.0: автоматизоване обладнання, сенсорний контроль та інформаційні системи дозволяють застосовувати автоматизоване управління підприємством. Ключові процеси контролюються дистанційно, та не вимагають втручання людей. Це дозволило прискорити процеси та виключити помилки, пов'язані з людським фактором та оптимізувати роботу персоналу.

Інноваційні технології РГК Метрологічного центру дозволяють значно скоротити час повірки лічильників в десятки разів: за 3 хвилини тут повіряють 60 побутових лічильників, тоді як раніше на повірку такої партії лічильників витрачалось майже 2,5 години [4].

Висновки. В роботі показано на скільки новітні технології впроваджені в процес скорочують час виконання завдання а разом з цим і затрати на дану роботу. В еру новітніх технологій усім компаніям в світі потрібно розвивати підприємства автоматизуючи, оптимізуючи та удосконалюючи виробництво. Чим більше підприємств буде зволікати з цим рішенням тим важче їм буде конкурувати з іншими підприємствами. Ідея Інтернету речей здатна кардинально вплинути на розвиток сучасного світу, оскільки дозволить багатьом виробничих процесів відбуватися без участі людини. У найближчому майбутньому Інтернет речей значно трансформує бізнес і навіть цілі галузі. Ця система допоможе вирішити цілий ряд глобальних проблем сучасного виробництва.

Література

1. Aramis: Загальна автоматизація українських підприємств – крок назустріч індустрії 4.0. - <http://aramis.com.ua/vseobshhaya-avtomatizatsiya-ukrainskih-predpriyatiy-shag-navstrechu-industrii-4-0/>.
2. Павленко В. І., Сітало І. А., Буць Д. Є. (2020) ІНТЕРНЕТ РЕЧЕЙ. ІНДУСТРІЯ 4.0. https://openarchive.nure.ua/bitstream/document/14078/1/Pavlenko_271-275.pdf.
3. IT-Enterprise: Промисловий Інтернет Речей - <https://www.it.ua/ru/knowledge-base/technology-innovation/promyshlennyj-internet-veschej>.
4. 2020/07/06 eba: В Україні побудували перший повністю автоматизований РГК Метрологічний центр - <https://eba.com.ua/v-ukrayini-pobuduvaly-pershyj-povnistyu-avtomatyzovanyj-rgk-metrologichnyj-tsentr/>.

ДОСЛІДЖЕННЯ СХЕМИ ADAPTIVE DATA RATE В ПРОТОКОЛІ ПЕРЕДАЧІ ДАНИХ LORAWAN

Міночкін Д.А., Рибак О.О.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: alex96.rybak@gmail.com

STUDY OF THE ADAPTIVE DATA RATE SCHEME IN THE LORAWAN DATA TRANSFER PROTOCOL

Long Range Wide Area Network (LoRaWAN) is a fast growing communications system for low power wide area networks (LPWAN) in Internet of Things (IoT) deployments. LoRaWAN is designed to optimize LPWAN for battery life, capacity, range and cost. LoRaWAN uses an Adaptive Data Rate (ADR) scheme that dynamically optimizes data rate, airtime and power consumption.

Схема Adaptive Data Rate (ADR) (адаптивна швидкість передачі даних) була розроблена для протоколу LoRaWAN, щоб мати можливість керувати параметрами передачі кінцевих вузлів для покращення доставки пакетів. Метою цієї схеми є мінімізація енергоспоживання та максимізація пропускної здатності шляхом коригування швидкості передачі даних в залежності від бюджету каналу зв'язку для кожного кінцевого вузла в мережі LoRaWAN. ADR управляє параметрами передачі, а саме: пропускною здатністю (BW), коефіцієнтом розширення (SF), потужністю передачі (TP) і швидкістю кодування (CR). Оптимізація ADR збільшує пропускну здатність мережі, так як пакети даних, що передаються з різними SF, можуть прийматися одночасно, що скорочує ефірний час. ADR - це механізм, який контролює параметри висхідної передачі повідомлень (UL) пристроїв LoRa в залежності від бюджету каналу. Функціональність ADR повинна бути включена на кінцевому вузлі, щоб її можна було використовувати. У реалізаціях LoRa, описаних в літературі, схеми ADR реалізуються і оцінюються з використанням різних підходів, таких як математичні моделі і моделювання. Основною проблемою алгоритму ADR є те, що специфікація LoRa не вказує спосіб, яким мережевий сервер (NS) повинен інструктувати кінцеві вузли щодо адаптації швидкості передачі даних [1]. Різке збільшення числа впроваджень IoT призводить до різних вимог до якості обслуговування (QoS) та підходів до реалізації, що створює проблему з точки зору надійності та придатності схем ADR.

У разі фіксованих кінцевих вузлів NS управляє ADR в залежності від історії отриманих UL пакетів, званої "ADR, керований по мережі, або Static ADR". Мережевий ADR підхід не працює для рухомих кінцевих вузлів, так

як загасання каналу відбувається в міру переміщення пристрою. Що стосується рухомих кінцевих вузлів, то ADR виконується "наосліп" на стороні кінцевого вузла, відомої як "сліпий ADR". У мережах LoRaWAN використовуються методи адаптивної модуляції з багатоканальними, багато модемними прийомо-передавачами на шлюзі для отримання безлічі повідомлень від каналів. Кожен конкретний сигнал використовує унікальний SF, з ортогональним поділом, забезпечуваним спектром. Ця техніка дає переваги в управлінні швидкістю передачі даних [2]. Схема ADR LoRaWAN динамічно адаптує параметри передачі з метою продовження терміну служби батареї і максимізації пропускної здатності. Це здійснюється шляхом зміни швидкості передачі даних і TP для кожного кінцевого вузла в мережі LoRa. ADR покращує швидкість передачі даних, ToA і енергоспоживання. У LoRaWAN зміна SF регулює швидкість передачі даних для кінцевих вузлів, оптимізуючи таким чином пропускну здатність. Проте, ADR слід використовувати з обережністю, так як на ймовірність зіткнення, яка безпосередньо впливає на пропускну здатність, впливає зміну SF [3]. Схема ADR заснована на виборі швидкості передачі даних з урахуванням минулих параметрів повідомлення кожного кінцевого вузла. Рівень MAC LoRaWAN містить чотири різні команди для ADR, які показані в таблиці 1.

Таблиця 1. Команди LoRaWAN Adaptive Data Rate (ADR).
NS: Мережевий сервер, UL: висхідний канал.

Команда	Опис
ADR	Кінцевий вузол встановлює даний біт, запитуючи у NS швидкість передачі даних
ADR = 1	NS буде контролювати швидкість передачі даних кінцевих вузлів
ADR = 0	NS не контролюватиме швидкість передачі даних кінцевих вузлів
ADRACKReq	Дозволяє кінцевим вузлам періодично отримувати підтвердження того, що NS отримує повідомлення UL
ADRACKReq = 1	NS повинен відповідати на підтвердження отримання даних
ADRACKReq = 0	Підтвердження отримання даних UL не потрібно.
LinkADRReq	Передається NS для запиту кінцевого вузла на зміну параметрів передачі
LinkADRAns	Передається вузлами у відповідь на команду LinkADRReq
LinkADRAns = 1	Параметри передачі успішно встановлені
LinkADRAns = 0	Команда відкляється

У мережах LoRaWAN контроль ADR дозволяє підтримувати з'єднання з мережею, забезпечуючи численні швидкості передачі даних. Стан радіочастотного з'єднання визначається станом прийому пакета ACK в LoRaWAN через помилки з'єднання. Це, однак, не вказує на перевантаженість мережі, але може привести до неефективної передачі даних через тривалі затримки передачі. Оскільки перевантаженість не рахується проблемою підключення, зниження швидкості передачі даних шляхом заміни системи модуляції недоцільно. Запропонована схема ADR розпізнає рівні

перевантаженості мережі шляхом прогнозованого навчання і подальшого застосування результату для управління швидкістю передачі даних. Як характеристик для навчання в методі використовуються швидкість передачі даних, RSSI, SNR і кількість з'єднань на шлюзі. Оцінка цих характеристик забезпечує оцінку перевантаженості мережі. Коли прогнозується перевантаження, запропонований алгоритм змінює час прийому замість зниження швидкості передачі даних, коригуючи затримку замість зниження пропускної здатності. Це призводить до підвищення точності управління швидкістю передачі даних і ефективності мережі. NS виконує навчання і передає результати на кінцеві вузли для прогнозування перевантажень. Розрахунки для навчання виконуються в NS. Сильною стороною цього підходу є те, що він враховує рівень перевантаженості мережі на відміну від успадкованої схеми ADR. Недоліком цього підходу є те, що процес вимагає отримання ACK DL повідомлення для кожної передачі. Оскільки трафік DL негативно впливає на пропускну здатність UL, PDR в результаті зменшується [4]. У подальших дослідженнях можна було б розглянути вивчення розподіленого навчання кінцевих вузлів для прогнозування затримок можуть бути застосовані й інші методи оптимізації.

Висновок. У специфікації LoRaWAN не вказано, як мережевий сервер повинен інструктувати кінцеві вузли щодо адаптації швидкості передачі даних. Це призвело до пропуску в реалізації ADR, оскільки схеми адаптації даних не досліджувались детально. Тому схеми ADR все ще актуальні для дослідження та моделювання. З огляду на сильні і слабкі сторони існуючих схем ADR, це прокладає шлях до розробки більш ефективних і дієвих алгоритмів. Дослідження показало, що хоча параметри передачі є стандартними, методи і міркування ADR щодо поліпшення продуктивності мережі незліченні. Були виявлені нові шляхи по оптимізації ADR. Незважаючи на те, що існуючі рішення досягли багатообіцяючої продуктивності, вони не є оптимальними, тому необхідно продовжити дослідження оптимізації ADR.

Література

1. Raza, U.; Kulkarni, P.; Sooriyabandara, M. Low power wide area networks: An overview. *IEEE Commun. Surv. Tutor.* 2017, 19, 855–873.
2. Alliance, L. LoRaWAN 1.0. 3 Specification; LoRa-Alliance: Boston, MA, USA, 2018; Volume 1, pp. 1–72.
3. El Fehri, C.; Kassab, M.K.; Abdellatif, S.; Berthou, P.; Belghith, A. LoRa technology MAC layer operations and Research issues. *Procedia Comput. Sci.* 2018, 130, 1096–1101.
4. Marais, J.; Malekian, R.; Abu-Mahfouz, A.M. Evaluating the lorawan protocol using a permanent outdoor testbed. *IEEE Sens. J.* 2019, 19, 4726–4733.

СИСТЕМА ВІДДАЛЕНОГО КЕРУВАННЯ ДОСТУПОМ

Тарновський А.М., Коляда К.В.

Факультет прикладної математики КПІ ім. Ігоря Сікорського, Україна

E-mail: tarnovski0211@gmail.com

REMOTE ACCESS CONTROL SYSTEM

An approach to building a system for remote access control for the hotel is proposed. The identifier for access is a QR code sent to the customer's mobile phone. The interaction between the administrator application and the access controller is carried out through the cloud server

Запропоновано підхід до побудови системи для віддаленого керування доступом для готелю. Ідентифікатором для доступу є QR-код, що надсилається на мобільний телефон клієнта. Взаємодія між додатком адміністратора та контролером доступу здійснюється через хмарний сервер.

Однією з перспективних сфер застосування систем контролю і управління доступом є готельний бізнес. Система контролю і управління доступом для готелів є сучасним інструментом, що дозволяє суттєво підвищити рівень безпеки і сервісу, зробити перебування гостя максимально комфортним, забезпечити режим енергоефективності та енергозбереження, тощо [1]. Як правило, сьогодні в готельних системах керування доступом використовуються електронні замки з доступом за безконтактною картою Em Marin або Mifare [2].

Розвиток та широке застосування Інтернет технологій у сфері готельного бізнесу характеризується впровадженням і поширенням Інтернет-бронювання. Багато готелів розміщують на своїх веб-сайтах (а також на сайтах туристичних компаній або фірм-посередників) модуль онлайн-бронювання, за допомогою якого відвідувач може самостійно вибрати номер і замовити його. У зв'язку з цим для повноцінної зручності бажано мати можливість отримувати права доступу до заброньованого номеру на визначений період також дистанційно. Особливо це актуально для малих готелів, в яких стійка реєстрації відсутня або працює не цілодобово.

Підходи до реалізації системи віддаленого керування доступом.

Сучасним трендом інформатизації в різних областях стало широке використання смартфонів. За допомогою смартфона можна отримати доступ до Інтернету, електронної пошти, банківських рахунків і багато чому іншому. Смартфон також може використовуватися і як засіб ідентифікації.

На теперішній час більшість систем контролю та управління доступом, що використовують технології мобільної ідентифікації, як правило містять чотири структурні компоненти [3]:

1. Мобільний ідентифікатор – цифровий код, що передається

бездротовим зв'язком від смартфона до зчитувача; його можна розглядати як віртуальну карту, що зберігається на смартфоні;

2. Мобільний зчитувач – пристрій для зчитування мобільного ідентифікатора і передачі його номера в контролер системах контролю та управління доступом;

3. Мобільний додаток – засіб для отримання і зберігання мобільного ідентифікатора, а також для здійснення взаємодії з мобільним зчитувачем;

4. Портал адміністратора – «хмарний» сервіс або додаток для персонального комп'ютера, що служить для видачі / відкликання мобільного ідентифікатора на смартфон.

У більшості випадків мобільна ідентифікація реалізується за допомогою інтерфейсу NFC. Проте такий підхід вносить суттєві обмеження щодо використання через відсутність підтримки NFC поки ще у більшості смартфонів. Тому отримання доступу за технологією NFC на теперішній час для багатьох клієнтів буде технічно не здійсненною.

З іншого боку, передачу коду між смартфоном та контролером доступу можна здійснити через Bluetooth. Не зважаючи на наявність Bluetooth майже в усіх мобільних телефонах такий підхід теж не можна вважати вдалим. По-перше, перше підключення мобільного телефону до контролера вимагає від користувача виконання певних дій для авторизації. Це потребує хоча і доволі незначного, але все ж таки певного рівня розуміння процесу та досвіду в здійсненні підключення через Bluetooth. По-друге, мобільний телефон за версією підтримуваного Bluetooth може виявитися не сумісним з тим, що підтримується контролером, а підтримка усіх можливих версій не є доцільною.

З врахуванням викладеного вище для отримання прав доступу пропонується здійснювати ідентифікацію за QR-кодом, що відображається на екрані смартфона. Такий підхід не висуває ніяких особливих вимог до характеристик мобільного телефону та технічної обізнаності користувача. Єдине що потрібно зробити, то це лише відкрити зображення коду на телефоні та піднести його до контролера.



Рис. 1. Система віддаленого керування доступом.

Структурно система віддаленого керування доступом складається з чотирьох компонентів: хмарного сервера, контролера доступу, додатка адміністратора та мобільного телефону клієнта (рис. 1).

Контролер доступу є мікроконтролерним засобом зі зчитувачем QR-кодом та Wi-Fi модулем. Обмін даними між контролером та додатком адміністратора, що задає ідентифікатор доступу у вигляді QR-коду, здійснюється за моделлю клієнт-сервер через хмарний сервер та точку доступу до бездротової мережі Wi-Fi відповідно до протоколу TCP/IP. Для побудови контролера може бути використаний мікроконтролері середньої продуктивності та модуль зчитувача QR-коду типу EM2028 [4] та Wi-Fi модуль типу ESP-07 [5].

Клієнт завантажує картинку з QR-кодом за URL посиланням, що надсилається йому адміністратором. Альтернативно код клієнту може бути надісланий через будь-який месенджер, наприклад, Viber або Telegram.

Висновки. Застосування Інтернет технологій популяризує Інтернет-бронювання, що робить бажаним отримання прав доступу віддалено. Це особливо актуально для малих готелів, в яких стійка реєстрації відсутня або працює не цілодобово.

Віддалене надання прав доступу може бути забезпечене за допомогою ідентифікатора, що надсилається на мобільний телефон. Простим рішенням ідентифікації з використанням мобільного телефону є ідентифікація за QR-кодом, яка, на відміну від ідентифікації через Bluetooth або NFC, може бути реалізована на будь-якому телефоні і вимагає від користувача лише елементарних навичок користування смартфоном.

Література

1. Система контроля и управления доступом для гостиниц. [Електронний ресурс]. Режим доступу: <https://avectis.by/solutions/integrirovannye-sistemy-bezopasnosti/sistema-kontrolya-i-upravleniya-dostupom-dlya-gostinic>.
2. Быков О. Системы контроля доступа на бесконтактных смарт-картах Mifare // Алгоритм Безопасности. 2011. № 3. С. 78 –79.
3. Умнов А. В. Системы мобильного доступа. Как сделать правильный выбор? // Алгоритм Безопасности. 2019. № 1. С. 32 –34.
4. Сканирующий модуль Newland EM2028. [Електронний ресурс]. Режим доступу: <https://agrovesy.com.ua/p1243145426-skaniuyuschij-modul-newland.html>.
5. Wi-Fi модуль ESP8266 версія ESP-07. [Електронний ресурс]. Режим доступу: <https://arduino.ua/prod1444-wi-fi-modul-esp8266-versiya-esp-07>.

СЕРТИФІКАЦІЯ КІБЕРБЕЗПЕКИ ІОТ: СИСТЕМА ТА СХЕМИ ОЦІНКИ ВІДПОВІДНОСТІ

Піхота К.В., Горицький В.М.

*Інститут телекомунікаційних систем КІП ім. Ігоря Сікорського, Україна
E-mail: pihotka19.11@gmail.com*

IOT CYBER SECURITY CERTIFICATION: SYSTEM AND CONFORMITY ASSESSMENT SCHEMES

Cybersecurity certification of IoT components plays an important role in the field of cybersecurity. The creation of IoT cybersecurity certification systems and schemes on the basis of cross-border recognition is currently an urgent task for Ukraine. The report considers the main aspects of ensuring the recognition of the results of certification on the basis of international agreements of Ukraine on the recognition of the results of accreditation of conformity assessment bodies.

Важливу роль у сфері кібербезпеки відіграє сертифікація кібербезпеки компонентів ІоТ. Створення систем та схем сертифікації кібербезпеки ІоТ на засадах транскордонного визнання на сьогодні є актуальним завданням для України. В доповіді розглянуті основні аспекти забезпечення визнання результатів сертифікації на основі міжнародних угод України щодо визнання результатів акредитації органів з оцінки відповідності.

Кібербезпека інформаційних та комунікаційних технологій (далі – ІКТ) сьогодні визнана ключовою проблемою для збереження функціонування та безпеки цифрової економіки і державного управління в найближчому майбутньому [1, 2].

Важливу роль у сфері ІКТ відіграє оцінка відповідності (сертифікація) кібербезпеки ІКТ [3]. Це може відноситись до кібербезпеки компонентів, продуктів, обладнання, послуг та процесів ІКТ, до кібербезпеки хмарних сервісів, до кібербезпеки технологічних процесів, до особистої компетентності у сфері кібербезпеки тощо. Кібербезпека пристроїв ІоТ та механізмів їх використання у цьому переліку також займає важливе місце.

Правила, процедури та менеджмент проведення сертифікації кібербезпеки встановлюють схему сертифікації, а набір правил та процедур для управління подібними або спорідненими схемами оцінки відповідності утворюють систему сертифікації [4].

В статті розглядається важлива та актуальна для сьогодення України задача - розробка системи та схем сертифікації для (ІоТ) на основі існуючої в Україні системи технічного регулювання та досягнень в сфері оцінки відповідності та акредитації [5], а також вимог діючого законодавства України у сфері кібербезпеки, яке встановлює завдання на застосування кращих міжнародних та європейських принципів оцінки відповідності інформаційної та кібербезпеки [1].

Оцінка відповідності – це демонстрація того, що «зазначені вимоги» (specified requirement), які стосуються продукції, процесу, послуги, системи,

особи чи органу, були виконані (оцінка відповідності включає такі види діяльності, як випробування, інспектування, валідація, верифікація, сертифікація та акредитація). «Зазначена вимога» – потреба або сподівання, яке зазначено (ці вимоги можуть бути викладені в нормативних документах, таких як регламенти, стандарти та технічні специфікації). Об'єкт, до якого застосовуються ці «зазначені вимоги» є об'єктом оцінки відповідності. Схема оцінки відповідності – це набір правил та процедур, що описує об'єкти оцінки відповідності, визначає ці вимоги та забезпечує методологію проведення оцінки відповідності. Схемою з оцінки відповідності можна керувати в рамках системи оцінки відповідності. Система оцінки відповідності (conformity assessment system) – набір правил та процедур для управління подібними або спорідненими схемами оцінки відповідності. Оцінка відповідності встановленим вимогам неупередженою третьою стороною, яка називається органом з оцінки відповідності (ООВ), називається сертифікацією [4].

За останні десятиліття у світі була створена безліч систем та оціночних стандартів, які застосовуються для сертифікації інформаційної та кібербезпеки. Найбільш відомими серед них є: стандарти сімейства ISO/IEC 27000; стандарти сімейства IEC 62443; Framework v1.1 Національного інституту стандартів і технологій (NIST) США; стандарт COBIT-5; ISO/IEC 15408; ISO/IEC 18045:2008; FIPS - 140 – США та інші.

Практичне застосування названі системи та стандарти сертифікації знаходять здебільшого в галузевих схемах сертифікації. Таке різноманіття створює потужні технічні бар'єри у широкому чи транскордонному визнанні відповідних оцінок (сертифікатів). Крім того, у більшості випадків існування або використання різних вимог і процедур у тих секторах, які функціонують як глобальні і комплексні системи, може саме по собі являти собою підвищений ризик.

В роботі запропоновано створювати систему сертифікації кібербезпеки IoT на механізмах національної системи технічного регулювання, з опорою на міжнародні угоди Національного органу України з акредитації органів з оцінки відповідності та ієрархічній моделі оціночних стандартів Системи сертифікації кібербезпеки, запропонованій в [7].

У сучасному глобалізованому світі, з метою усунення технічних бар'єрів для визнання оцінок відповідності та сертифікатів, сформована глобальна система з оцінки відповідності, яка створює умови для взаємного визнання оцінок відповідності та сертифікатів. Ця система, – акредитація органів з оцінки відповідності (ООВ), до яких відносяться й органи з сертифікації [6].

У структурі технічного регулювання орган, відповідальний за акредитацію, оцінює компетенцію органів з сертифікації продукції, послуг та процесів, систем менеджменту, інспектування й персоналу, випробувальних й калібрувальних лабораторій. Офіційне визнання, іменоване акредитацією, засвідчує клієнтам і користувачам послуг компетентність діяльності даних організацій. Акредитація може забезпечити транскордонне визнання своїх

послуг в рамках Міжнародного форуму з акредитації (IAF) і Міжнародного комітету з акредитації лабораторій (ILAC) [8,9].

IAF і ILAC сприяють й управляють визнанням Двосторонніх або Багатосторонніх Угод або Домовленостей (MRA/MLA), згідно з якими сторони, які беруть участь в них, погоджуються обопільно визнавати результати тестування, інспекцій, сертифікації або акредитації. Угоди MRA/MLA сьогодні стали важливим кроком на шляху оптимізації чи зменшення числа сертифікацій продуктів, послуг, систем, процесів і матеріалів, необхідних особливо в міжнародній діяльності [8,9].

На рисунку 1 представлено рівні та сфери, за якими в глобальній системі IAF визнано національний орган акредитації України.



Рис. 1. Угода MRA та сфера в IAF.

Слід також додати, що глобальні системи IAF/ILAC діють через регіональні організації з акредитації, які входять до цих систем. Їх географічна локація зображена на рис. 2 та 3.

Для України регіональною організацією з акредитації є Європейська організація з акредитації (EA) [10].

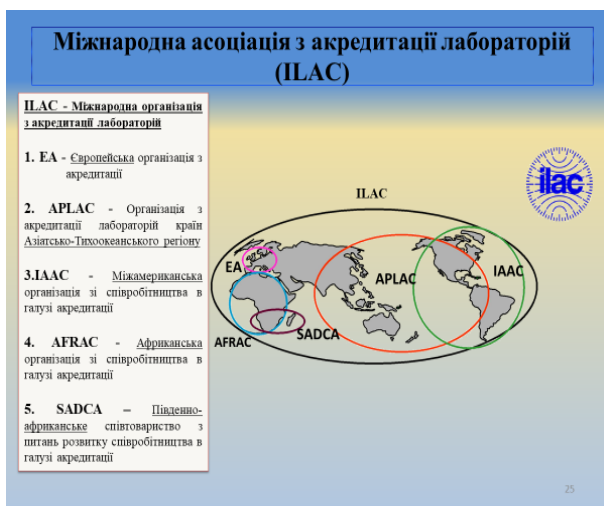


Рис. 2. Регіональні організації ILAC.

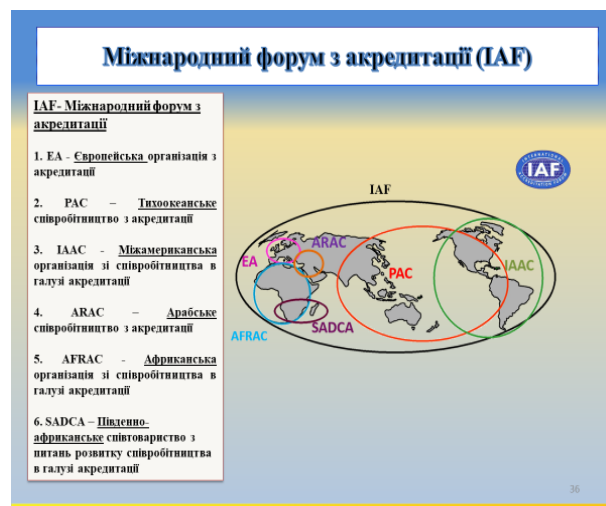


Рис. 3. Регіональні організації IAF.

Висновки. Сертифікація кібербезпеки IoT потребує в цілях транскордонного визнання результатів сертифікації розробки відповідних схем та систем сертифікації.

Схеми сертифікації IoT в Україні можуть бути побудовані на механізмах національної системи технічного регулювання, з опорою на міжнародні угоди Національного органу України з акредитації органів з оцінки відповідності.

Література

1. Про основні засади забезпечення кібербезпеки України Закон України від 05.10.2017 № 2163-VIII // Відомості Верховної Ради України. – 2017. № 45.
2. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації Розпорядження Кабінету Міністрів України; від 17.01.2018 № 67-р. – Режим доступу : <https://www.kmu.gov.ua/npas/pro-shvalennya-konceptiyi-rozvitku-cifrovoyi-ekonomiki-ta-suspilstva-ukrayini-na-20182020-roki-ta-zatverdzhennya-planu-zahodiv-shodo-yiyi-realizaciyi>
3. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) – [Чинний від 2019-04-17]. – Режим доступу: <https://eur-lex.europa.eu/eli/reg/2019/881/oj>.
4. Conformity assessment - Vocabulary and general principles : ISO/IEC 17000:2020. – [Чинний від 2020-01-06]. – International Organization for Standardization/International Electrotechnical Commission, 2020. – 30 P.
5. Про технічні регламенти та оцінку відповідності Закон України від 15.01.2015 № 124-VIII // Відомості Верховної Ради України. – 2015. – № 14.
6. Про акредитацію органів з оцінки відповідності Закон України від 17.05.2001 № 2407-III // Відомості Верховної Ради України. – 2001. – № 32.
7. Цвілій О.О. ІЄРАРХІЧНА МОДЕЛЬ ОЦІНОЧНИХ СТАНДАРТІВ СИСТЕМИ СЕРТИФІКАЦІЇ КІБЕРБЕЗПЕКИ ІКТ. DOI: 10.24412/9215-0365-2021-59-1-54-58. <http://www.scientific-heritage.com/wp-content/uploads/2021/02/VOL-1-No-59-59-2021.pdf>
8. International Accreditation Forum [Електронний ресурс]. – Режим доступу: <https://www.iaf.nu/>.
9. International Laboratory Accreditation Cooperation [Електронний ресурс]. – Режим доступу: <https://ilac.org/>.
10. European co-operation for Accreditation [Електронний ресурс]. – Режим доступу: <https://european-accreditation.org/>

ОЦІНКА ВІДПОВІДНОСТІ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ: АКРЕДИТАЦІЯ ОРГАНІВ З ОЦІНКИ ВІДПОВІДНОСТІ

Кочева Н.В., Горицький В.М.

Інститут телекомунікаційних систем КПП ім. Ігоря Сікорського, Україна

E-mail kocheva.nadia@gmail.com; gorytski@ukr.net

CONFORMITY ASSESSMENT OF ELECTRONIC TRUST SERVICES: ACCREDITATION OF CONFORMITY ASSESSMENT BODIES

With the adoption in 2017 of the Law of Ukraine "On electronic trust services" and a number of bylaws, there is a need to create in Ukraine a system for assessing the conformity of facilities, processes and organizations that provide electronic trust services. The article considers ways to harmonize such a system for assessing compliance with EU requirements set out in Regulation (EU) No 910/2014 (eIDAS), identifies problems and suggests ways to address them.

З прийняттям у 2017 році Закону України «Про електронні довірчі послуги» та низки підзаконних актів є потреба створення в Україні системи оцінки відповідності об'єктів, процесів та організацій, що надають електронні довірчі послуги. У статті розглядаються шляхи гармонізації такої системи з оцінки відповідності до вимог ЄС, викладених в *регламенті (ЄС) №910/2014 (eIDAS)*, визначаються проблеми та пропонуються шляхи їх усунення.

Регламент (ЄС) eIDAS забезпечує нормативно-правову базу для електронної ідентифікації та довірчих послуг для електронних транзакцій на європейському цифровому ринку. Одним з суттєвих рішень в eIDAS є вимога акредитації органів з оцінки відповідності (ООВ) надавачів довірчих послуг [1]. При цьому Регламент eIDAS застосовує визначення органів з оцінки відповідності з іншого регламенту (ЄС), - Reg.765/2008, де встановлені вимоги до акредитації ООВ та ринкового нагляду. *Регламент (ЄС) 765/2008 визначає ООВ як «орган, який здійснює діяльність з оцінки відповідності, включаючи калібрування, тестування, сертифікацію та перевірку»*. У контексті Регламенту eIDAS ООВ є органом, визначеним вище, який додатково акредитований як компетентний для проведення оцінки відповідності провайдерів кваліфікованих довірчих послуг та кваліфікованих довірчих послуг вимогам Регламенту eIDAS. Щоб отримати кваліфікований статус, провайдери довірчих послуг повинні продемонструвати, що вони відповідають вимогам, встановленим у регламенті eIDAS, пройшовши процес оцінки відповідності. Цей процес проводиться акредитованим органом з оцінки відповідності (ООВ) eIDAS.

Регламент eIDAS не вказує схему акредитації або будь-яку схему оцінки відповідності, за якою ООВ повинен бути акредитований. Це призводить до різноманітних схем оцінки відповідності, що використовуються ООВ і впливає на якість наданих ними оцінок. З метою гармонізації цього процесу Європейська Комісія може, шляхом імплементації актів відповідно до ст.20(4) eIDAS, встановити ряд довідкових стандартів (reference standards) щодо

акредитації ООВ та правил аудиту, за якими ООВ проводитиме їхню оцінку відповідності [1].

Важливим є також те, що в ЄС створена і ефективно діє інфраструктура оцінки відповідності та акредитації, яка використовується в різних сферах, включаючи eIDAS.

Відповідно до статті 32 Закону «Про електронні довірчі послуги» в Україні повинна проводитись оцінка відповідності у сфері електронних довірчих послуг, яка гармонізована у повній відповідності до положення eIDAS [2]. Підзаконний акт, що в певній мірі деталізує ці вимоги, - постанова Кабінету Міністрів України від 7 листопада 2018 року № 992 «Про затвердження вимог у сфері електронних довірчих послуг та порядок перевірки додержання законодавства у сфері електронних довірчих послуг», де визначений стандарт ДСТУ ETSI EN 319 403:2016 “Електронні підписи та інфраструктури (ESI). Оцінювання відповідності провайдерів довірчих послуг. Вимоги до органів з оцінювання відповідності, що оцінюють провайдерів довірчих послуг” [3].

Також постановою Кабінету Міністрів України від 18 грудня 2018 р. № 1215 впроваджено «Порядок проведення процедури оцінки відповідності у сфері електронних довірчих послуг», який встановлює механізм проведення процедури оцінки відповідності вимогам до кваліфікованих надавачів електронних довірчих послуг та послуг, що ними надаються [4].

Разом з тим, на сайті центрального засвідчувального органу України (Міністерство цифрової трансформації України) досі відсутні відомості про акредитовані згідно статті 32 Закону органи з оцінки відповідності у сфері електронних довірчих послуг, що пройшли акредитацію в національному органі з акредитації [5]. Цієї інформації немає і на сайті національного органу з акредитації України, - Національного агентства з акредитації України [6].

Такий стан свідчить про складність та актуальність задачі впровадження системи *оцінки відповідності постачальників довірчих послуг* на засадах ЄС та необхідність її вирішення в найкоротші терміни.

В статті досліджено механізми акредитації органів з оцінки відповідності у сфері електронних довірчих послуг та шляхи їх впровадження в діяльність відповідних суб'єктів та об'єктів України.

Діяльність з акредитації ООВ, яка відповідає вимогам Європейського регламенту № 765/2008 в Україні покладено на Національний орган з акредитації - Національне агентство з акредитації України (НААУ) [7].

НААУ на сьогодні визнане в ЄС (Європейською кооперацією з акредитації - EA) та в усьому світі на рівні Угод про визнання та є членом ряду міжнародних та регіональних організацій з акредитації (міжнародні організації з акредитації ILAC та IAF). Зокрема, Європейської співпраці з акредитації (EA) та підписантом двосторонньої угоди про визнання (EA BLa).

Регіональні організації Міжнародного форуму з акредитації IAF, повноправним членом яких є НААУ, представлені на Рис 1 [9].

Загальна модель Угод про визнання результатів в акредитації, підписантом яких є НААУ, представлена на Рис. 2 [10].



Рис. 1. Регіональні організації IAF.

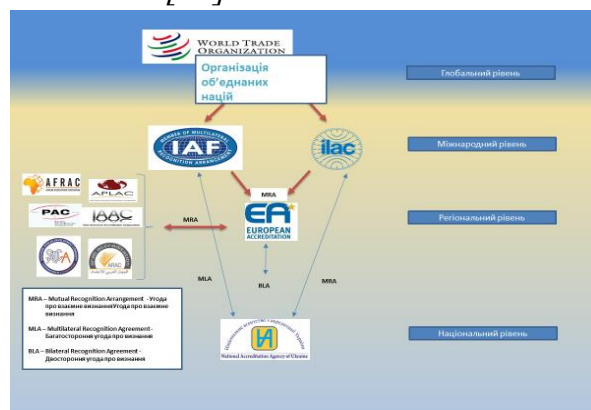


Рис. 2. Модель Угод MRA/MLA.

На рис. 3 показано Угоду про співробітництво НААУ з ЕА. Актуальні сфери акредитації, які підпадають під Угоду НААУ з ЕА знаходяться на сайті ЕА [8].

EA EUROPEAN ACCREDITATION

Extension of Bilateral Agreement

NAAU (BLA) National Accreditation Agency of Ukraine UKRAINE

SCOPE OF RECOGNITION		EA MLA Council decision date
EA MLA Level 2: Activity	EA MLA Level 2: Standard	
Testing	EN ISO/IEC 17025	19 April 2012
Certification	EN ISO/IEC 17025	19 April 2012
Inspection	EN ISO/IEC 17020	8 October 2014
Product certification	EN ISO/IEC 17050	2 October 2015
Certification of persons	EN ISO/IEC 17024	3 October 2015
Management system certification	EN ISO/IEC 17021	19 April 2012

Walter Goryshko
Acting Chairman of NAAU

Nicola Morio-Vanathem
Chair of EA MLA Council

Рис. 3. Зміст Угоди НААУ з ЕА.

Багатостороння угода ЕА (ЕА МЛА) - це підписана угода між членами ЕА, згідно з якою підписанти визнають і приймають еквівалентність систем акредитації, що експлуатуються членами підписання, а також надійність результатів оцінки відповідності, наданих органами з оцінки відповідності (ООВ), акредитованими членами, що підписали.

Таким чином, акредитація ООВ в сфері довірчих послуг повинна бути здійснена таким чином, щоб це відповідало вимогам eIDAS з одного боку, а з іншого, - можливостям (сфері визнання в ЕА) НААУ.

В даний час існують різні схеми і програми, що вимагають акредитації для довірчих послуг на: EN 45011; ISO/IEC 17021 для надання сертифікації відповідно до ISO 27001 (з виконанням ISO 27006); ISO 20000; Webtrust. Разом з тим, всі існуючі в ЄС домовленості передбачають перехід до акредитованої оцінки по TS 119 403, а потім EN 319 403.

Проміжні заходи для цього були задокументовані на Генеральній асамблеї ЕА у 2014 році і передбачали, що будь-який орган з оцінки відповідності, який в даний час пропонує акредитовану сертифікацію на основі вищезазначених критеріїв, може продовжувати надавати цю послугу до дати завершення акредитації (липень 2016 року) за умови, що:

– Орган з оцінки відповідності має демонстрований досвід в діяльності з оцінки відповідності послуг TSP вимогам політики ETSI або аналогічним критеріям (наприклад, Webtrust) або ISO 27001 або ISO 20000.

– Орган з оцінки відповідності має задокументований міграційний план акредитації по EN 319 403. Заявка на акредитацію повинна бути зроблена в належний час для того, щоб орган з акредитації надав акредитацію в терміни до липня 2016 по схемі ISO/ IEC 17065 + TS 319 403, а до вересня 2016 здійснити перехід від TS 119 4xx до EN 319 4xx, шляхом перегляду документації.

– Всі TSPs будуть сертифіковані на TS 119 4xx до липня 2017, а до липня 2018 - на EN 319 4xx.

Слід зазначити, що НААУ має визнання в ЕА у сфері ISO/IEC 17065. Крім того, в Україні відсутні акредитації ООВ для довірчих послуг для будь якої наведеної вище схеми.

Таким чином, на сьогодні потрібною та достатньою для України схемою акредитації для ООВ довірчих послуг повинна бути ISO/IEC 17065+EN 319 403.

Це ще потребує певних зусиль для НААУ, ООВ та технічного регулятора в цій сфері, що буде досліджено в майбутньому.

Висновки. *Загалом система оцінки відповідності в Україні відповідає європейській.* Огляд існуючих методів та систем оцінки відповідності для електронних довірчих послуг дозволяє зробити рекомендації щодо вдосконалення систем акредитації і оцінки відповідності для електронних довірчих послуг України у відповідності до регламенту ЄС eIDAS.

Відсутність певних інституційних елементів в інфраструктурі оцінювання України має бути вирішена найближчим часом.

Література

1. Електронний ресурс: Регламент (ЄС) № 910/2014 «Про електронну ідентифікацію та довірчі послуги для електронних транзакцій в межах внутрішнього ринку та про скасування Директиви 1999/93/ЄС», [режим доступу: EUR-Lex - 32014R0910 - EN - EUR-Lex (europa.eu)].
2. Закон України «Про електронні довірчі послуги» від 5 жовтня 2017 року № 2155 - VIII, Голос України, 2017, № 206.
3. *Постанова Кабінету Міністрів України від 7 листопада 2018 року № 992 «Про затвердження вимог у сфері електронних довірчих послуг та порядок перевірки додержання законодавства у сфері електронних довірчих послуг».*
4. Постанова Кабінету Міністрів України від 18 грудня 2018 р. № 1215 впроваджено «Порядок проведення процедури оцінки відповідності у сфері електронних довірчих послуг».
5. [<https://czo.gov.ua/>].
6. [<https://naau.org.ua/reystar-akreditovanix-oov/>].
7. Про акредитацію органів з оцінки відповідності Закон України від 17.05.2001 № 2407-III // Відомості Верховної Ради України. – 2001. – № 32.
8. European co-operation for Accreditation [Електронний ресурс – Режим доступу: <https://european-accreditation.org/>].
9. International Accreditation Forum [Електронний ресурс – Режим доступу: <https://www.iaf.nu/>].
10. Цвілій О.О. Ієрархічна модель оціночних стандартів системи сертифікації кібербезпеки ІКТ. DOI: 10.24412/9215-0365-2021-59-1-54-58. [<http://www.scientific-heritage.com/wp-content/uploads/2021/02/VOL-1-No-59-59-2021.pdf>].

SEMINAR
Modern information and telecommunication trends

UDC621.37

**RESEARCH OF ALGORITHMS OF
SERVICE OF LOADINGS IN FOG – NETWORKS**

MoshynskaA.V., SozonnikG.D., MaltsevA.G.

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: maltsev.andrew@gmail.com; avmoshinskaya@gmail.com

**ДОСЛІДЖЕННЯ АЛГОРИТМІВ ОБСЛУГОВУВАННЯ
НАВАНТАЖЕНЬ У FOG – МЕРЕЖАХ**

У роботі представлено основні принципи забезпечення автоматизованої роботи та оптимізації бездротових мереж при використанні самооптимізуючих систем (SON) за допомогою туманних мереж.

Wireless networks are and will continue to be a fundamental cornerstone of the global digital economy and our connected society, provisioning diverse services for people and things. The proliferation of smart user devices, such as smart phones, laptops, and tablets, is pushing the current wireless networks to their limits. Wireless networks are experiencing an unprecedented traffic growth with an estimated compound annual growth rate of 0.6-1.0 and an increasing variety of services and applications, each with potentially different traffic patterns and quality of service (QoS) and quality of experience (QoE) requirements, for example, ultra-high data rate and/or reliability, and ultra-low latency. To cope with the continuing traffic growth and service expanding, future wireless networks will have to be heterogeneous and densely deployed, featuring the coexistence of different radio access technologies (RATs), such as LTE/LTE-advanced, Wi-Fi, IoT, 5G NR, etc. Wireless network self-optimization comprises various mechanisms that optimize network parameters during operation according to measurement data taken at different parts of the network.

Fog computing, also called Edge Computing, is intended for distributed computing where numerous "peripheral" devices connect to a cloud. (The word "fog" suggests a cloud's periphery or edge). Many of these devices will generate voluminous raw data (e.g., from sensors), and rather than forward all this data to cloud-based servers to be processed, the idea behind fog computing is to do as much processing as possible using computing units co-located with the data-generating devices, so that processed rather than raw data is forwarded, and bandwidth requirements are reduced. An additional benefit is that the processed data is most likely to be needed by the same devices that generated the data, so that by processing locally rather than remotely, the latency between input and response is minimized.

A self-organizing network (SON) is an automation technology designed to make the planning, configuration, management, optimization and healing of mobile radio access networks simpler and faster. SON functionality and behavior has been defined and specified in generally accepted mobile industry recommendations produced by organizations such as 3GPP (3rd Generation Partnership Project) and the NGMN (Next Generation Mobile Networks).

Nevertheless, most existing SON solutions are mainly based on heuristics, with the automated information processing limited to relatively simple methods [2]. Many open challenges of SON remain unsolved, for example, the automated coordination between different SON functions, and the trade-off between centralized and distributed SON implementations.

Fog computing can be used to enhance the operations, administration, and maintenance (OAM) processes for distributed MLB in support of multi-RAT coordination.

Wireless networks are and will continue to be a fundamental cornerstone of the global digital economy and our connected society, provisioning diverse services for people and things.[1] Different network architectures have been considered for the realization of SON, including centralized SON, distributed SON, and hybrid SON. The choice of the SON architecture may affect the performance and/or efficiency of the SON functionalities for wireless networks.

In centralized SON (C-SON), the self-optimizing algorithms mainly reside in the network management system (NMS). In distributed SON (D-SON), the SON functions are distributed across the edge of the network, typically in BSs and APs.

Hybrid SON (H-SON) combines the centralized network management and the distributed SON functionalities.

Mobility load balancing (MLB) is a self-optimization function that aims to maximize the network capacity (or to optimize user QoS or QoE) through optimizing the distribution of user traffic load across the network nodes and radio resources. As a result, traffic overload or congestion at any network node can be avoided. MLB is usually implemented in a distributed manner and relies on the traffic load estimation and radio resource utilization status exchanged among neighboring network nodes via the X2 interface.

For last several years wireless networks used offloading to edge servers. The main benefit of offloading to edge servers is that it can support real-time tasks by providing low latency connectivity for the application on mobile devices. The problem arises when there are a number of mobile devices in hot spots. In such a scenario, multiple devices try to access nearby edge servers, which have limited capabilities compared to the central cloud server. When a load balancing technique is not applied, some edge servers are prone to failures. However, implementing a load balancing technique for edge servers in edge cloud computing environments is not an easy task, and a few load balancing techniques are implemented for edge servers; previous load balancing techniques are mainly for virtual machine or container consolidation Electronics 2020, 9, 686 3 of 13 and orchestration in the central cloud server. Thus, we design and implement a load balancing technique in edge cloud computing environments with graph coloring based on a genetic

algorithm.

But now, using FOG – computing there are much more ways of offloading. Such as Genetic Algorithms.

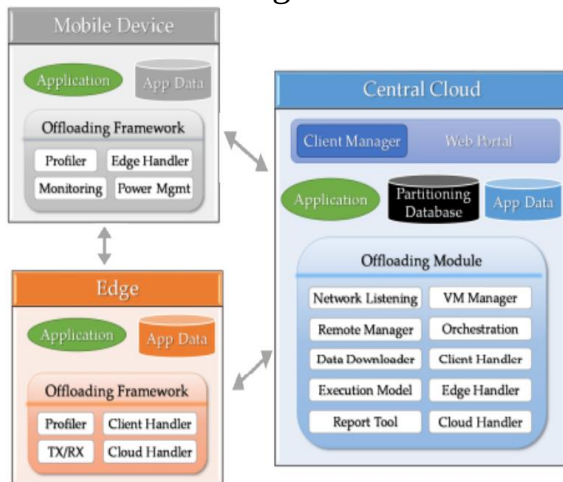


Fig.1. An edge cloud architecture and its interaction.

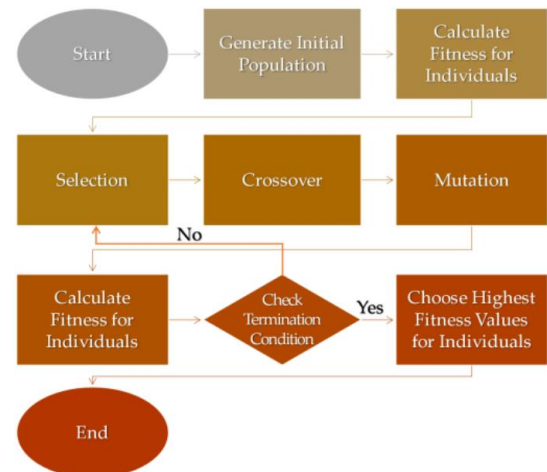


Fig.2. The process of a genetic algorithm.

To mimic natural evolution processes, it reflects the natural selection process with a fitness function for individuals and produces the next generation based on crossover and mutation processes. Figure 3 shows the process of a genetic algorithm. It starts with the initial population of the genesis generation and uses of a genetic algorithm. It starts with the initial population of the genesis generation and uses a fitness function to measure scores for individuals in the population. Then, it selects a target based on the fitness function and process the crossover and mutation processes to mimic the evolutionary process of humans.

Specifically, a genetic algorithm can be used to solve optimization problems for large datasets and search space.

Conclusions. The advantages of employing a genetic algorithm are as follows.

Firstly, it can solve fundamental problems with global maxima and minima.

Secondly, it can handle complex mathematical representations with low complexity, while the linear programming approach exhibits high complexity.

Thirdly, it supports problems that are difficult to represent in mathematical forms. Fourthly, it is resilient to data noise and failures.

Fifthly, it is easy to implement solutions by exploiting parallel and distributed processing.

Lastly, it can learn with new data and information in a continuous fashion to achieve global maxima and minima.

References

1. Bonomi F, Milito R, Zhu J, Addepalli S (2012) Fog computing and its role in the Internet of things. In: Proceedings of the first edition of the MCC workshop on mobile cloud computing, Helsinki, August 2012, pp 13-16.
2. Lopez-Perez D, Guvenc I, Chu X, Mobility management challenges in 3GPP heterogeneous networks. IEEE Commun Mag, 2012, pp 70-78.
3. Mao Y, Zhang J, Letaief KB, Dynamic computation offloading for mobile-edge computing with energy harvesting devices. IEEE J Sei Areas Commun, 2016, pp 3590-3605.

IOT-SYSTEM DEVELOPMENT FOR ENERGY METERS DATA TRANSFER AND PROCESSING

Loboda R., Osypchuk S.

*Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: serg.osypchuk@gmail.com*

РОЗРОБКА ІОТ-СИСТЕМИ ПЕРЕДАВАННЯ ТА ОБРОБКИ ДАНИХ ПРО ВИКОРИСТАНІ ЕНЕРГОРЕСУРСИ

В роботі представлено результат практичної реалізації проекту Інтернету речей для автоматизованого збору телеметрії, а саме – збору і обробки показників приладів обліку енергоресурсів (води, газу, тепла, електрики, тощо), які по замовчуванню не оснащені інтерфейсом для передавання даних в телекомунікаційну мережу. Зібрані дані доступні в мережі Інтернет.

The paper presents the result of IoT automated telemetry collection project practical implementation, namely – data collection and processing from energy meter devices (water, gas, heat, electricity, etc.). The energy meters in focus of this work are not equipped by default with the data transmission interface. Collected data from such energy meters are available in the Internet.

Problem statement. There is a large number of homes and enterprises where IoT data collection, specifically – from various energy meters (**EM**), – is not automated and requires manual data pulling from those EMs (water, gas, heat, electricity, etc.), because such EMs are not equipped with an interface for data transmission to telecommunication network. As a result, the data transfer process from EMs to data collection centers requires regular and significant human resources involvement, while this process is pretty out of sync with time, and involves the errors likelihood due to the human factor presence in the data collection process. In current work, one of the options for solving this problem is presented, namely – implementation of custom data transmission system for EMs that are not equipped with any data transmission interface by default.

It is important to note that an alternative solution to this problem is to replace the EM with a more modern EM that has a telecommunication interface by design, e.g. pulse type – for data collection and transmission from that EM to data center. However, replacing EM which doesn't have a telecommunication interface, with another EM which is equipped with some telecommunication interface by design, requires both significant material resources and bureaucratic efforts to reissue documents for EM. Therefore, a large number of people are not ready for such costly EM upgrade.

Therefore, in scope of this work, the decision was made to analyze possible solutions for this problem, develop a cost-effective solution and implement a

testbed system that can automatically collect data from EMs which don't have telecommunication interface by default and require human visual look for data collection, and transmit values to data center via telecommunications network, without replacing existing EMs with a new one. First steps of this effort were done in [1] and continued in this work.

Data collection and transmission system. The telecommunication device with photcamera (TCPC) was developed in the work for the use with EMs, which is a supplement to EM. Such TCPC does not require intervention in the design of EM and is installed as a nozzle on top of EM. TCPC is based on a telecommunication module with a photcamera (model ESP32Cam [2]), which performs the function of photographing the visual appearance of EM and sending photos to the data center via WiFi / Internet. The TCPC fastening to EM is designed and manufactured on a 3D printer for suitable attachment TCPC on some EM. To obtain a better quality photo by TCPC, the additional lighting is used based on LED. In this work, experiments with TCPC were performed on two experimental meters, cold and hot water (Fig. 1).

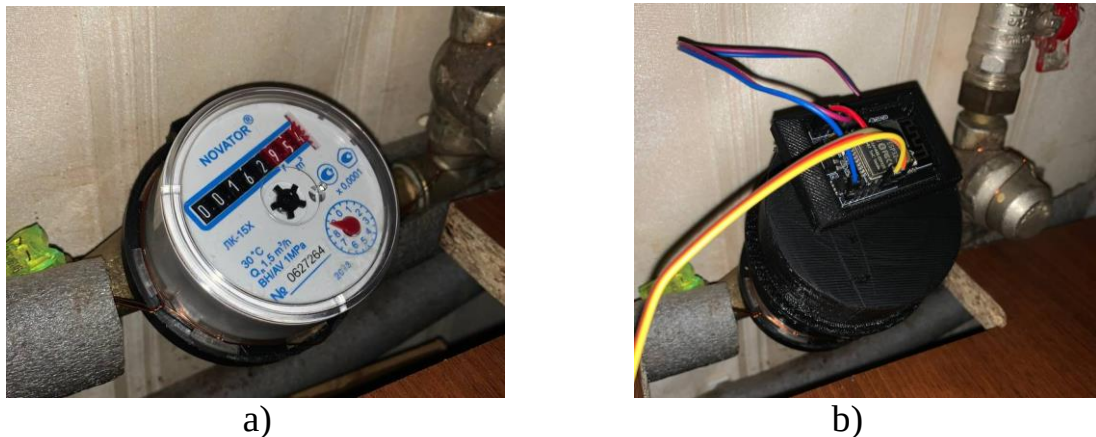


Fig. 1. Photos of EM before (a) and after (b) TCPC installation on EM.

The TCPC work principle is shown on diagram (Fig. 2): photos taking of EM values with a certain time interval, photos transferring through a WiFi network to data center, and their placement to web server. In this experiment, the data center is represented by a computer unit with a properly configured software that accepts images when they are sent from TCPC; then it stores photos on a storage and web-server shows them on the website [3]. Accordingly, each EM has its own data set on a website.

Web page has the following functionality: the main page displays a list of all EMs from which data are sent by TCPC (Fig. 2,a), and through the link in the list you can go to any of the EMs to view the EMs values from photos (Fig. 2,b). Images from EMs are sorted sequentially by creation date.

It is important to highlight that the WiFi telecommunication interface used in TCPC can be replaced by any other wireless (preferably high-speed for photo transmission) or wired interface. The system can also be easily scaled to a large EMs number, so can suit both personal and industrial needs.

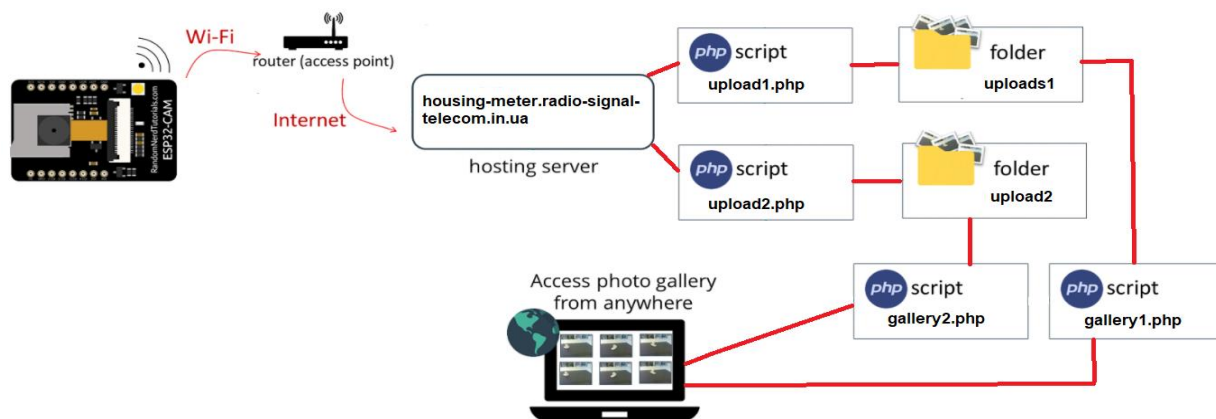


Fig. 2. The TCPC solution work principle: automated data collection from EMs to data center and its web presentation.

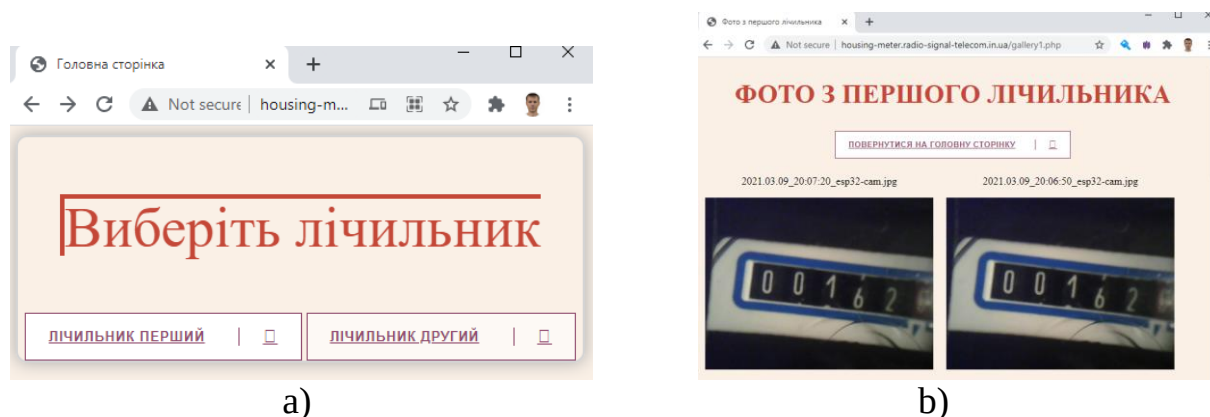


Fig. 3. Web page with EMs list (a) and web page with data available on the Internet from first EM.

Thus, the testbed of automatic data collection and transmission to data center on the basis of TCPC, from EMs without the built-in telecommunication interface, is developed and demonstrated. The advantage of this proposed solution is ~50-70% lower cost of implementation compared to the replacement by new EMs with a telecommunication interface, and the need absence to reissue documents on new EM. The disadvantage of propose solution is the need in a custom configuring TCPC for a given EM in each case.

References

1. L. Uryvsky, W. Gerstacker, A. Moshynska, S. Osypchuk, O. Yatsyshyn. RESEARCH AND IMPLEMENTATION OF IOT PROJECTS FOR ENVIRONMENT PARAMETERS AND ENERGY RESOURCE METERING. – ISSN 2312-4121, Information and Telecommunication Sciences, 2020, Volume 11, Number 1. – 2020, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”. – pp. 1-4.
2. Telecommunication device with camera, model ESP32Cam – <https://randomnerdtutorials.com/esp32-cam-video-streaming-face-recognition-arduino-ide/>.
3. Web-page for tested energy meters in scope of this work – <http://housing-meter.radio-signal-telecom.in.ua/>.

FOG-NETWORK WITH SMART CONTROL SYSTEM MODEL DEVELOPMENT

Piavchyk M., Budishevskiy O., Osypchuk S.

*Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: serg.osypchuk@gmail.com*

РОЗРОБКА МОДЕЛІ FOG-МЕРЕЖІ З ІНТЕЛЕКТУАЛІЗОВАНОЮ СИСТЕМОЮ УПРАВЛІННЯ

В даній роботі запропонована архітектура мережі FOG з інтелектуальною системою управління (ІСУ). Акцентовано, що забезпечення технологій IoT обумовлює зростання об'єму трафіку та його флуктуацій, в той час як цей трафік повинен бути оброблений з мінімальними затримками з метою прийняття правильних рішень на основі вмісту IoT-трафіку, що виконує ІСУ.

In this paper the FOG network architecture with smart control system (SCS) is proposed. It is emphasized that the provision of IoT technologies causes traffic increase and fluctuations, while this traffic must be processed with minimal delays in order to make the right decisions based on the IoT traffic content. Decision making is performed by SCS.

Introduction. The paper considers one of the world trends in the modern infocommunication technologies development – *FOG* network [1]. In this work, the FOG network is a tool to ensure functioning of another technological trend – Internet of Things (*IoT*) [2].

Since the development of big data and computing networks, several distributed computing paradigms have emerged: *Clouds*, *FOG*, and *Edge*. The *FOG* paradigm takes the position *in the middle between* Cloud and Edge; while being as close as possible to *Edge* devices, and FOG partially has the same properties of data storage and computing properties as *Cloud* has. Collecting data from IoT devices and processing those data in FOG network allow *preventing* certain situation, *managing* it, or *regulating* its consequences as quickly as possible.

FOG is defined as a *decentralized* computing infrastructure in which *data*, *computing units*, and *applications* take place *between cloud* and *data sources*, and the resources of such network are used to *store* and *process* data, with access to data locally and over the Internet. FOGs are characterized by proximity to end users, pooling local resources, reduction of delays and capacity savings of the backbone network.

Limited network, storage and computing *resources* necessitate the creation of an efficient and optimal system for managing such resources – *smart control system* (SCS), which will manage requests and data from IoT devices by *expanding*

or *reducing* network resources, or *keeping* the current amount of computing resources required to process incoming traffic.

Model description. This paper proposes a *model of FOG network*, which involves transporting data from IoT sensors to FOG network and to SCS, processing information in SCS, and making decisions in SCS on the impact on *FOG network resources* and the on the *control object (CO)* (Fig. 1).

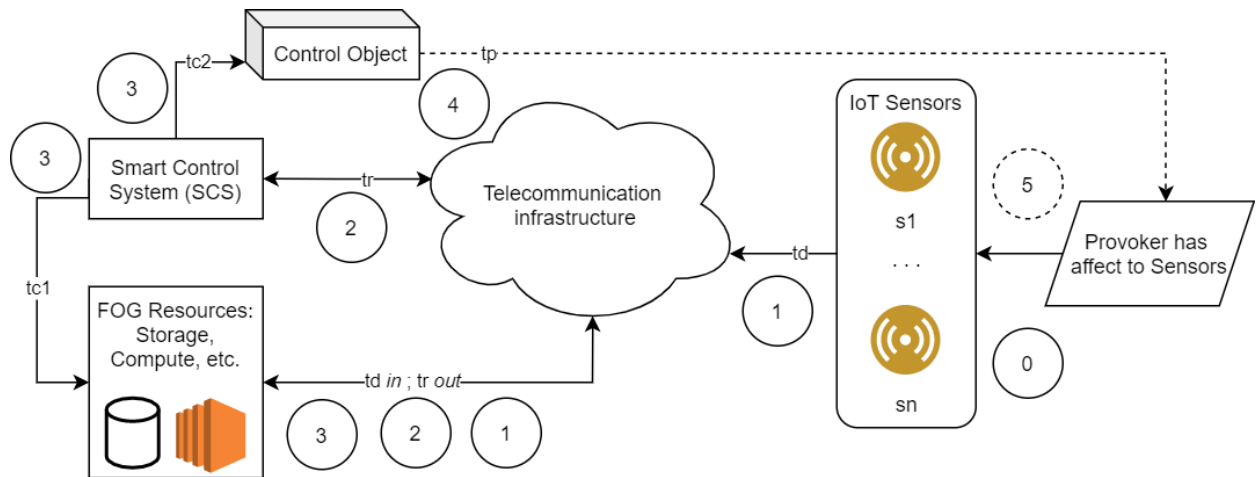


Fig. 1. The FOG network scheme with a smart control system (SCS).

Let us review the proposed FOG network model functionality step-by-step.

Step 0. Suppose there is a specific pathogen that affects IoT sensors.

Step 1. Incoming traffic from sensors $s_1, \dots, s_n$, with some specified characteristics and parameters:

- number of sensors: n ,
- sampling the time of sending data from one sensor: td ,
- amount of data sent from one sensor: Vd .

TC Infrastructure (TCI) provides communication between sensors and FOG resources, SCS, CO.

Vs data from IoT sensors is written to the *storage resources* of the FOG network for further retention and processing.

Storage resources of FOG network have a certain limited total capacity S , bytes.

Step 2. SCS analyzes the collected information Vs at intervals tr . SCS attracts or releases the computing resources of the FOG network to provide a necessary computational capacity for analyzing the received data from sensors.

It is important to note that the *computational resources* of the FOG network have a limited performance P , Instructions Per Second (IPS) [3]. The calculations speed in FOG network is influenced by the factor of *calculation complexity* [4]. The *calculations complexity* is influenced by the *incoming traffic type and its*

characteristics [5].

Step 3. SCS receives the information from FOG network and makes a decision on the instructions transmission need to the control object CO at discrete intervals: $tc1$, $tc2$. CO can be:

- *Computing resources of the FOG network*, to attract more or release computing resources for the purpose to process the required amount of data for decision-making by SCS,
- *Other management facilities* that may respond to an event or emergency in an appropriate manner (fire, military, medical, etc.)

Step 4. Response of the CO to the received information at discrete time intervals tp . For example, such a response may be the implementation of actions caused by notifying the nearest locations of fire brigades, informing public services about the increased radiation background in the region, responding to an increase in enemy military forces in the region, and so on.

Step 5. As a result of performing actions to respond to the received information, it is expected that in Step 0, but *in subsequent cycles*, the *pathogen may have a modified effect* on IoT sensors, which will lead to *other decisions in the SCS*.

Conclusion. As shown, the proposed algorithm for the operation of the FOG network with SCS provides:

- *generating traffic* with certain characteristics by IoT sensors,
- *storing and processing data* in the FOG network,
- *SCS implementation* for making decisions on the FOG-network resource and control objects management, while enabling learning mechanism for SCS based on the IoT traffic flow, decisions made, and reached effect to control objects,
- establishing *relationships* between *incoming IoT traffic* and its impact on the *decision* to perform an action or omission on the *control object*.

The next step in this work is to create a *simulation model* according to the proposed scheme of the FOG-network with an *intelligent control system* and discover its behavior when changing the input parameters. The *proposed model* can be used for *different needs of national, local or corporate importance*, in order to effectively respond to changes in the environment.

References

1. FOG networking: [https://en.wikipedia.org/wiki/Fog_computing].
2. Internet of Things: [https://en.wikipedia.org/wiki/Internet_of_things].
3. Instructions per second: [https://en.wikipedia.org/wiki/Instructions_per_second].
4. Computational complexity: [https://en.wikipedia.org/wiki/Computational_complexity].
5. Network traffic: [https://en.wikipedia.org/wiki/Network_traffic].

TRENDS AND FUTURE OF CLOUD TECHNOLOGIES IN GAMING INDUSTRY

Bidukha D.O., Pravylo V.V.

*Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: denys.the.angry.human@gmail.com*

ПЕРСПЕКТИВИ ТА МАЙБУТНЄ ХМАРНИХ ТЕХНОЛОГІЙ В ІНДУСТРІЇ ВІДЕО-ІГОР

Доповідь містить короткий огляд на поточні досягнення та історію розвитку в області хмарного геймінгу, технології що використовуються для забезпечення роботи хмарних сервісів, переваги і недоліки даних технологічних рішень для користувачів, складності в розвитку цього напрямку та перспективи і вимоги до сервісів на найближче та віддалене майбутнє.

This article briefly describes the actual achievements and the history of cloud gaming development. The authors will overview the technologies that were used to ensure work of the services, pros and cons of decisions made in this sphere for users, peculiarities of trends and future development of cloud services and cloud gaming in particular.

Cloud computing is the availability of resources via any means of remote communication. The most data are transmitted over the Internet. A lot of work and especially data are stored in outsource servers and data centers. For business it brings reliability as remote storages and computing resources protect the workflow from any downtime or blackouts. Meanwhile, for users the perks are not so obvious, they may vary from sphere to sphere, so particular cloud gaming is to be discovered in the article [1].

Traditional means of gaming is something, wherein a game is launched locally on user's console, personal computer, or mobile device. Cloud gaming is sometimes regarded as gaming on demand that runs games on servers and streams the image to user's device, in other words, it is playing a game in a cloud.

The pioneer of cloud gaming technology idea was the global corporation called G-cluster which demonstrated it at E3 in 2000 [2]. The developers offered service used over Wi-Fi to handheld devices. This idea was not taken seriously and didn't get any support. With development of broadband internet more service providers started thinking if they could connect a user to a game launched on their services without making gamers download the software. Residents of Ukraine as well as other Eastern-Europe citizens might have seen the advertisements starting year 2015 about services that offer a possibility to play "demanding to resources" games using a low-tear hardware. The only thing needed was the reliable internet connection. Most of them had no-name and had much technical trouble. That was a

reaction for loud start of such platforms on the west: in USA and Europe. Yet there was lack of availability in CIS (The Commonwealth of Independent States), the services were limited strictly in a number of countries. Most popular platforms such as GeForce Now and Google Stadia released in 2015 (2017 for PC) and 2019 respectively.

For cloud gaming services - significant infrastructure is required for the service to work as intended such as data centers and server farms to store the resources for games and high-bandwidth internet connections that also requires low latency to stream the image to users. As for the users – vice versa – it relieves common gamers from being forced to update their computers and have any difficulties with setting the game to work properly.

Having the Google Stadia as an example of the mark of the situation shows that despite of much internet service providers progress – yet the latency is not satisfying. The ping via service may vary from 50 or 500 milliseconds while a user of a PC or console should have 5 to 15 milliseconds. There is a list of other differences to consider: ownership, price, availability. In services like Google Stadia, a system of subscription works: if you stop paying monthly, you lose all the purchased in-store goods. Yet this may be fixed by using a bound Steam account. The price for this service is just 10 USD/monthly that saves you from buying a 1000 USD personal computer or 500 USD gaming console. Especially when the prices for GPU are rising constantly. Last but not least is availability. Not everyone has a reliable internet-connection, while offline is not an option for any cloud technology. Yet an autonomic device may be handled where you can access electricity. Laptops have even more autonomy in the last case [3,4].

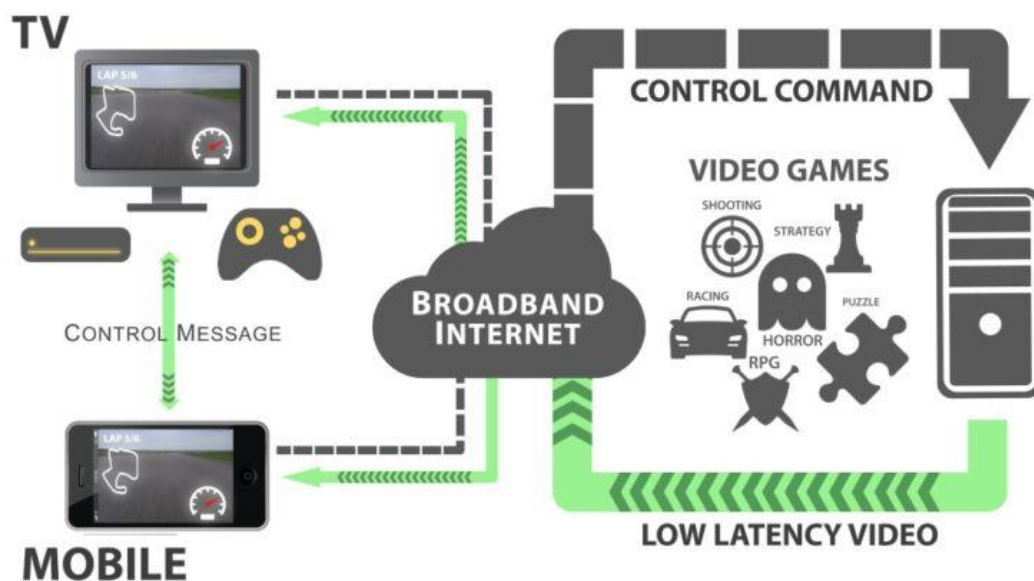


Fig.1. Schematic of cloud gaming.

There is also a different type of cloud tech presented world-wide. The most popular virtual video-game store launched their own app for mobile devices called Steam Remote Play that uses your PC as a server and your phone as a controller (command input) and video output [5]. This decision seems really good for single-player games as your phone is connected to your home means that server is not far from you. With availability of 4G in the underground it gives users an opportunity to connect to home PC computing resources from their smartphone being anywhere in the city.

To sum up, the cloud technologies are rapidly developing and becoming more and more popular. Casual gamers with low-tier devices and mobile users may rent services to play for a reasonable price, while for hardcore gamers there is a possibility to play their favorite titles via Google Stadia and Steam Remote Play. On the other hand, it is available only within stable internet connection and has no autonomy from subscription (except for Steam Remote Play that is free) [6].

All the servers have similar aims for the future. To make possible GPU resource sharing and predict user's input. Today most services have a GPU dedicated to each person playing a game. The idea is to schedule its resources with the purpose to improve streaming scalability. Another algorithm developed to predict player's input. That must overcome the impact of latency in cloud gaming applications. The last one can even bring some applications to "negative latency" where an action is done even before the input was made.

In conclusion, it is important to note that the cloud gaming market is growing much faster than it was predicted. In 2016 its general value was 56 million USD. By year 2019 it grew up to 512 million and in 2021 it is going to pass the mark of a billion value. We can see that this industry is developing rapidly and have a lot to cover in future. Cloud computing might be a great solution for a range of tasks in the nearest future.

References

1. P. P. Ray, "An Introduction to Dew Computing: Definition, Concept and Implications," in *IEEE Access*, vol. 6, pp. 723-737, 2018, doi: 10.1109/ACCESS.2017.2775042.
2. "Cloud gaming streaming services set to change your game - Latest News | Gadgets Now". *Gadget Now*. 2019-10-27. Retrieved 2019-10-28.
3. H. Yadav and B. Annappa, "Adaptive GPU resource scheduling on virtualized servers in cloud gaming," 2017 Conference on Information and Communication Technology (CICT), Gwalior, India, 2017, pp. 1-6, doi: 10.1109/INFOCOMTECH.2017.8340641.
4. Dobra, Andrei (April 27, 2009). "Crytek Attempted Cloud Gaming Way Before OnLive". *Softpedia*. Retrieved October 7, 2010.
5. K. Chen, Y. Chang, H. Hsu, D. Chen, C. Huang and C. Hsu, "On the Quality of Service of Cloud Gaming Systems," in *IEEE Transactions on Multimedia*, vol. 16, no. 2, pp. 480-495, Feb. 2014, doi: 10.1109/TMM.2013.2291532.
6. Lee, Kyungmin; Chu, David; Cuervo, Eduardo; Kopf, Johannes; Degtyarev, Yury; Grizan, Sergey; Wolman, Alec; Flinn, Jason (2015). "Outatime: Using Speculation to Enable Low-Latency Continuous Interaction for Mobile Cloud Gaming". *Proceedings of the 13th Annual International Conference on Mobile Systems, Applications, and Services - MobiSys '15*. Florence, Italy: ACM Press: 151–165. doi:10.1145/2742647.2742656. ISBN 978-1-4503-3494-5. S2CID 612942.

THE COHERENT DEMODULATION PROCEDURE OF MUTUALLY NON-ORTHOGONAL DIGITAL SIGNALS

Peleshok Y.V., Honenko S.V.*, Horlichenko S.O.

Institute of Special Communication and Information Protection

National Technical University of Ukraine

“Igor Sikorsky Kyiv Polytechnic Institute”

**E-mail: gonenko1995@gmail.com*

ПРОЦЕДУРА КОГЕРЕНТНОЇ ДЕМОДУЛЯЦІЇ ВЗАЄМНО НЕОРТОГОНАЛЬНИХ ЦИФРОВИХ СИГНАЛІВ

У роботі досліджується процедура когерентної демодуляції взаємно неортогональних цифрових сигналів з гаусівською мінімальною частотною маніпуляцією з метою повторного використання радіочастотного ресурсу.

The efficient use of radio frequency resources plays a crucial role in the world, considering that the social, economic and technical development of the country no less depends on the effectiveness of its use.

According to the Law of Ukraine “On Radio Frequency Resource of Ukraine”, the main principles of radio frequency resource management in Ukraine are: protection of radio frequency assignments; efficient use of distributed radio frequency bands; development of scientifically substantiated recommendations for making appropriate decisions to increase the efficiency of use and meet the needs of users of the radio frequency resource of Ukraine [1].

In order to reuse the radio frequency resource, it is proposed in this paper to use the methods of digital signal separation statistical theory to perform a synthesis of the non-orthogonal digital signals with Gaussian Minimum Shift Keying (GMSK) processing procedure.

The coherent demodulation procedure of mutually non-orthogonal digital signals with Gaussian minimum frequency manipulation has a number of advantages [2]:

- if the average power of the first GMSK signal is significantly exceeded over the power of the second GMSK signal and there are no errors in estimating the parameters of a stronger signal, and the potential noise immunity of the procedure is the same as in the absence of the first powerful signal;

- in the absence of the first GMSK signal, this procedure degenerates into a classical coherent demodulation of GMSK signal;

- this procedure can be used in the implementation of frequency resource reuse programs and in the development of promising interference-protected radio communications.

Despite the great variety of modulation types, methods, etc. in practice only a limited number of them can be used. Modern communication systems require special attention to the efficient use of resources such as transmission power and

channel bandwidth. According to these criteria, GMSK is well suited for mobile communication and is already implemented in GSM systems and IEEE 802.15 specification (Bluetooth), the used concept has the advantage that the information is transmitted in phase changes, rather than in the phase itself.

The GMSK signal can be easily detected using an orthogonal coherent detector, which is similar to the classic signal with Minimum Shift Keying (MSK).

GMSK modulation is based on MSK, which is a form of Continuous Phase Frequency Shift Keying (CPFSK). One of the problems with standard PSK forms is that the sidebands strongly expand out of the media. And we can use MSK and GMSK to overcome this. MSK as well as GMSK is implemented as a continuous phase circuit. There are no phase breaks, because the frequency changes occur at the points of zero carrier intersection. This is due to the unique quality for MSK and GMSK. Thus, the frequency difference between logic 0 and 1 states is always equal to half of the data rate. This can be expressed in terms of the modulation index equal to 0.5.

At the k -th clock interval, the signal is determined by the following formula:

$$s_i(r_{ik}, t) = A_i \cos(\omega_0 t + r_{ik} \Omega_\Delta t + \varphi_{ik} + \varphi_{i0}), t \in [t_{k-1}, t_k), \quad (1)$$

where A_i – amplitude of the signal with MSK, ω_0 – carrier frequency, Ω_Δ – frequency deviation, r_{ik} – discrete parameter (informational symbol), φ_{i0} – initial phase.

Thus, we see that the signal with MSK depends not only on the informational symbol on k -th clock interval but also on the previous values of it.

The MSK makes the phase change linear and limited to $\pm (\pi / 2)$ per bit interval T . This allows MSK to provide a significant improvement over the QPSK. Due to the effect of linear phase change, the power spectral density has weak side lobes that help control the interference of the adjacent channel. However, the main lobe becomes wider than in quadrature manipulation. Since we have the task of separating two signals, it will accordingly be necessary to represent both signals in such a way that it would be possible to record the observation of input and the likelihood functionals following it.

There are two main ways in which the GMSK signal can be generated. The most obvious way is to filter the modulating signal using a Gaussian filter, and then transmit it to the frequency modulator, where the modulation index is set to 0.5. This method is very simple, but it has a major drawback, which is that the modulation rate should be equal to 0.5 and in practice this method is not suitable, because certain values affect the signal and it is impossible to accurately set the modulation index.

The second method is more widely used and it consists in the fact of using a quadrature modulator that means the signal phase is quadrature or changed by 90 degrees relative to the initial. The quadrature modulator uses components, which are in-phase and the quadrature. Due to the phase and quadrature elements, this type of modulator is often called the I-Q modulator. Using this type of modulator,

the modulation rate can be maintained at exactly 0.5, without the need for additional settings. This makes it relatively easy to use and provide the required level of accuracy without the need for adjustment.

For demodulation, this technique is used in the opposite direction. Since the spectrum of the MSK signal in such scheme will also have side lobes extending beyond the bandwidth, it is necessary to reduce them by passing the modulating signal through the low-pass filter before applying it to the carrier. The requirements for the filter are: it must have a sharp limit, a narrow bandwidth, and its impulse response must not exceed.

The optimal filter known as a Gaussian filter has the Gaussian response to the pulse we need. Actually, by adding such a filter to the circuit, a GMSK signal is obtained.

The possibility of reuse of the radio frequency resource will be provided by building the model, which will be working with given conditions and providing the needed task, namely - ensuring the processing of two mutually non-orthogonal digital signals. To build a workable model, the mutual energies for these two signals will be calculated, one of which, provided, is more powerful than the other.

Its implementation is planned and already developing by using Matlab software package, Simulink application. Initially, for the case of ideal coherent receiving, it is necessary to synthesize a model that will operate on one clock interval, which, although will be losing in noise immunity to a signal from BPSK however still emerging a new quality, that is the ability to separate each of the signals in one radio channel operating simultaneously.

An important factor is to determine the noise immunity of this model, which is also possible in this software package, and the indicators that will be measured to evaluate it: Bit Error Rate (BER) and the signal-to-noise ratio (SNR). A high BER causes increased packet loss, increased latency, and reduced system bandwidth, and is the opposite of SNR [3]. The GMSK modem performance in many works is determined by measuring the SNR to BER.

Conclusion. Thus, this procedure allows using the same frequency band for both digital mutual non-orthogonal signals that is beneficial in the way of reusing the radio frequency resource. It is expected that the difference in power of 6 dB will allow the receiving side to separate two signals without loss of information. This will increase the number of subscribers operating simultaneously within one GSM cell, which will have a positive impact on the performance of the system as a whole.

References

1. Law of Ukraine “On Radio Frequency Resource of Ukraine” of June 1. 2000, № 1770. URL: <https://zakon.rada.gov.ua/laws/show/1770-14> (access date 23.03.2021).
2. Lupas L., Verdu S. “Linear Multiuser Detectors for Synchronous Code-Division Multiple-Access Channels” IEEE Trans. Information Theory Vol. IT-35, pp. 123–136, Jan. 1989.
3. Peer-reviewed technical communication: Estimating signal-to noise ratio (SNR) / B. T. Bosworth and others. IEEE Journal of Oceanic Engineering. 2008. Vol. 33, № 4. P. 414–418. DOI: 10.1109/JOE.2008.2001780.



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

**ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ
НДІ ТЕЛЕКОМУНІКАЦІЙ**

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

Присвячена Дню науки та Всесвітньому Дню телекомунікацій

15 квітня 2021 року

Тези конференції

м. Київ

ПРОГРАМНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ ПРІТС-2021

Співголови конференції:

ІЛЬЧЕНКО М.Ю. – 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;

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

УРИВСЬКИЙ Л.О. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;

ЛИСЕНКО О.І. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;

РОМАНОВ О.І. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;

ТРУБІН О.О. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;

СКУЛИШ М.А. - д.т.н., с.н.с., КПІ ім. Ігоря Сікорського, Київ;

МОШИНСЬКА А.В. - д.т.н., с.н.с., КПІ ім. Ігоря Сікорського, Київ;

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

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

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

КОНОНОВА І.В. – к.т.н., доц., 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;

Члени програмного комітету:

Авдеєнко Г.Л., ст. викладач, КПІ ім. Ігоря Сікорського, ІТС, Київ;

Валуйський С.В., к.т.н., доц., 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;

Кравчук І.М., ст. викладач, КПІ ім. Ігоря Сікорського, ІТС, Київ;

Штогриня О.С., к.т.н., КПІ ім. Ігоря Сікорського, ІТС, Київ.

Засідання 1.

АНАЛІЗ РОЗВИТКУ МОБІЛЬНИХ МЕРЕЖ П'ЯТОГО ПОКОЛІННЯ В УКРАЇНІ

Хижняк О. П. кер. Правило В. В.
Науковий консультант: **Правило В. В.**
Інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: hiz01072000alex@gmail.com

Проведено аналіз розвитку впровадження технологій п'ятого покоління в Україні на основі існуючих тестувань. Проаналізовано основні переваги та недоліки при розгортанні нового покоління мобільного зв'язку. Наведено діапазон частот, який буде використовуватись в Україні. Розглянуто вплив технології п'ятого покоління у сфері IoT, на прикладі керування розумним будинком та містом.

ANALYSIS OF THE DEVELOPMENT OF FIFTH GENERATION MOBILE NETWORKS IN UKRAINE

Khyzhniak O. P.
Scientific adviser: **Pravylo V. V.**
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: hiz01072000alex@gmail.com

An analysis of the development of the introduction of fifth generation technologies in Ukraine on the basis of existing tests. The main advantages and disadvantages of deploying a new generation of mobile communications are analyzed. The frequency range that will be used in Ukraine is given. The influence of the fifth-generation technology in the field of IoT, on the example of smart home and city management, is considered.

АНАЛІЗ ВРАЗЛИВОСТЕЙ І НЕДОЛІКІВ КІБЕРБЕЗПЕКИ В МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ

Хижняк С. П.

Науковий керівник: **Правило В. В.**

Інститут телекомунікаційних систем

КПІ ім. Ігоря Сікорського, Україна

E-mail: Khizhnyak56843@gmail.com

Як і будь-яка інша технологія, що розвивається, Інтернет речей має безліч переваг та ризиків. Пристрої Інтернету речей нові і люди можуть скористатися недоліками кібербезпеки зі злим умислом, тому безпека інтернету речей залишається головним пріоритетом. У цій роботі ми розглянемо кілька питань кібербезпеки, а також важливість збереження інформації від кібератак.

ANALYSIS OF CYBER SECURITY VULNERABILITIES AND DEFICIENCIES ON THE INTERNET OF THINGS

Khyzhniak S. P.

Scientific adviser: **Pravylo V. V.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: Khizhnyak56843@gmail.com

Like any other evolving technology, the Internet of Things has many benefits and risks. IoT devices are new and people can take advantage of the disadvantages of cybersecurity with malicious intent, so IoT security remains a top priority. In this paper, we will consider several issues of cybersecurity, as well as the importance of preserving information from cyber attacks.

АНАЛІЗ ТЕЛЕКОМУНІКАЦІЙНИХ FOG-ІНФРАСТРУКТУР ДЛЯ ОБСЛУГОВУВАННЯ ТРАФІКУ ІОТ

Нескородов В.В.

Науковий керівник: **Осипчук С.О.**

Інститут телекомунікаційних систем

КПІ ім. Ігоря Сікорського, Україна

E-mail: vlad.neskw@gmail.com

Технології ІоТ виконують цифрову трансформацію галузей, – розумне місто, виробництво, енергетика, тощо. Обчислення туману (Fog) підходять для обробки великих даних, які чутливі до часу, і генеруються засобами ІоТ. У даній роботі проведений аналіз та класифікація парадигми Fog-обчислень, і пов'язаних з нею обчислювальних парадигм на основі набору атрибутів. Виконано порівняння обчислювальних Fog-інфраструктур за комунікаційними, обчислювальними, та технологіями зберігання даних. Розглянуто Fog-стандарти як сучасні рекомендації щодо Fog-обчислень. Огляд телекомунікаційних технологій для Fog-мереж проведений за критеріями дальності та швидкості передачі даних.

FOG TELECOMMUNICATION INFRASTRUCTURES ANALYSIS FOR IOT TRAFFIC HANDLING

Neskorodov V.V.

Scientific adviser: **Osypchuk S.O.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: vlad.neskw@gmail.com

The IoT drives digital transformation of industries, e.g. smart cities, manufacturing, energy, etc. Fog computing is suitable for handling the big data that is being produced by the IoT, which is often time-sensitive. So, in this work the fog computing and related computing paradigms are analyzed and classified based on set of attributes. Comparison of fog computing infrastructures is performed focusing on communication, computing, and storage technologies. Fog standards are reviewed as modern recommendations in Fog computing. Telecommunication technologies review is performed for Fog networks by range and data rate criteria.

ЕВОЛЮЦІЯ МЕРЕЖ GPON ТА GE-PON

Тельчарова Д. О.

Науковий керівник: **Носков В. І.**

Інститут телекомунікаційних систем

КПІ ім. Ігоря Сікорського, Україна

E-mail: tennis080900@gmail.com

Досліджено технології пасивних оптичних мереж широкосмугового доступу GPON та GE-PON за стандартами МСЕ-Т та IEEE. Розглянуто основні поняття, загальний принцип функціонування та етапи подальшого еволюційного розвитку мереж доступу на основі PON.

EVOLUTION OF GPON AND GE-PON NETWORKS

Tielcharova D. A.

Scientific adviser: **Noskov V. I.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: tennis080900@gmail.com

The technologies of passive optical networks of GPON and GE-PON broadband access according to the ITU-T and IEEE standards have been studied. The basic concepts, the general principle of functioning and stages of further evolutionary development of access networks on the basis of PON are considered.

АНАЛІЗ СУЧАСНИХ СТАНДАРТІВ І ПЛАТФОРМ ДЛЯ ПОБУДОВИ ІОТ СИСТЕМ

Волох М.А.

Науковий керівник: **Міночкін Д.А.**

Інститут телекомунікаційних систем

КПІ ім. Ігоря Сікорського, Україна

E-mail: maxim.volokh0505@gmail.com

Напрямок ІоТ систем стрімко розвивається, тому на даний час уже є декілька платформ та стандартів для побудови даних систем. Але вибір правильної платформи або стандарту є важливим для побудови ІоТ систем. Тому розгляд та визначення чим вони між собою різняться вирішує проблеми правильної побудови цих систем.

ANALYSIS OF MODERN STANDARDS AND PLATFORMS FOR BUILDING IOT SYSTEMS

Volokh M.A.

Scientific adviser: **Minochkin D.A.**

Institute of Telecommunication System,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: maxim.volokh0505@gmail.com

The direction of IoT systems is developing rapidly, so now there are several platforms and standards for building these systems. But choosing the right platform or standard is important for building IoT systems. Therefore, consideration and determination of how they differ solves the problem of proper construction of these systems.

ТРАНСПОРТНІ МЕРЕЖІ НА ОСНОВІ ТЕХНОЛОГІЇ NG SDH

Паршин А.Ю.

Науковий керівник: **Носков В.І.**

Інститут телекомунікаційних систем

КПІ ім. Ігоря Сікорського, Україна

E-mail: antonparshyn@ukr.net

Розглянуті передумови появи транспортних мереж, побудованих за технологією SDH наступного покоління. Проаналізовані технічні принципи і відмінності технології NG SDH: віртуальна (VCAT - Virtual Concatenation) конкатенація віртуальних контейнерів; протокол управління перепускною здатністю каналу (LCAS – Link Capacity Adjustment Scheme); універсальний фрейм GFP-T.

TRANSPORT NETWORKS BASED ON NG SDH TECHNOLOGY

Parshin A.Y

Scientific adviser: **Noskov V.I.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: antonparshyn@ukr.net

Prerequisites for the emergence of transport networks built on NG SDH technology are considered. Technical principles and differences between NG SDH and original SDH technology are analyzed: virtual concatenation (VCAT); Link Capacity Adjustment Scheme (LCAS); GFP-T universal frame.

АНАЛІЗ ВПЛИВУ ВЛАСТИВОСТІ САМОПОДІБНОСТІ ТРАФІКУ НА ЯКІСТЬ ОБСЛУГОВУВАННЯ

Криклива А.В.

Науковий керівник: **Уривський Л.О.**

Інститут телекомунікаційних систем,

КПІ ім. Ігоря Сікорського, Україна

E-mail: kriklivanastya@gmail.com

На сьогоднішній день збільшується кількість користувачів, які працюють з інформацією через Інтернет. А отже і збільшуються можливості, які доступні для кожного, незалежно від місцезнаходження.

На прикладі хмарних обчислень в даній роботі розглянуті розрахунки показників якості обслуговування в системі масового обслуговування (СМО), за допомогою якої моделюється доступ до «хмари». Сформульована задача порівняння отриманих характеристик СМО в разі пуассонівського потоку заявок та з урахування самоподібності трафіку.

ANALYSIS OF THE INFLUENCE OF TRAFFIC SELF-SIMILARITY PROPERTIES ON THE QUALITY OF SERVICE

Krikliwa A.V.

Scientific adviser: **Uryvsky L.O.**

Institute of telecommunication systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: kriklivanastya@gmail.com

Today, the quantity of users who work with information via the Internet is increasing. Consequently, the opportunities available to everyone, regardless of location, are increasing.

In this paper on the example of cloud-computing calculations of quality indicators of the queuing system (QS) are considered. With the QS is modeled access to the Cloud. The problem of comparison of the received characteristics of QS with Poisson flow and with self-similarity traffic is formulated.

РОЗВИТОК АЛГОРИТМІВ ПІДВИЩЕННЯ ПРОПУСКНОЇ ЗДАТНОСТІ В МОБІЛЬНИХ СЕНСОРНИХ МЕРЕЖАХ

Бубка Б.А.

Науковий керівник: **Лисенко О.І.**
*Інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: sterbig18@gmail.com*

Розглядається загальна концепція поняття «сенсорна мережа» і структура сенсорної мережі. Розглядаються приклади використання сенсорних мереж і методи підвищення пропускної здатності БСМ. На основі математичної моделі сенсорної мережі проводиться оцінка різних протоколів рівня доступу до середовища стандарту ZigBee з точки зору ефективної пропускної здатності безпроводної сенсорної мережі. В роботі досліджуються 4 гіпотетичних способи підвищення пропускної здатності БСМ та один практичний спосіб. Дані методи підвищення пропускної здатності можуть бути використані в Україні у таких сферах, як воєнний і громадський зв'язок, моніторинг діяльності підприємств, моніторинг атмосферних явищ та інших сферах. Вибір того чи іншого методу підвищення пропускної здатності сенсорної мережі – індивідуальний і залежить від топології мережі, від програмно – апаратної реалізації, від часу експлуатації, від енергоефективності та енергозабезпеченості та від інших факторів.

DEVELOPMENT OF ALGORITHMS FOR INCREASING PERFORMANCE IN MOBILE SENSOR NETWORKS

Bubka B.A.

*Scientific adviser: Lysenko O.I.
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
Email: sterbig18@gmail.com*

The general concept of the concept of "sensor network" and the structure of the sensor network are considered. Examples of the use of sensor networks and methods of increasing the bandwidth of BSM are considered. Based on the mathematical model of the sensor network, various protocols for the level of access to the ZigBee standard are evaluated in terms of effective bandwidth of the wireless sensor network. The paper investigates 4 hypothetical ways to increase the bandwidth of BSM and one practical way. These methods of increasing capacity can be used in Ukraine in such areas as military and public relations, monitoring of enterprises, monitoring of atmospheric phenomena and other areas. The choice of one or another method of increasing the bandwidth of the sensor network is individual and depends on the topology of the network, on the software and hardware implementation, on the operating time, on energy efficiency and energy supply and other factors.

ТЕХНІЧНІ ПРИНЦИПИ ПЕРЕДАЧІ СИГНАЛІВ В МЕРЕЖАХ LTE

Березовський І. М.

Науковий керівник: **Носков В. І.**

Інститут телекомунікаційних систем

КПІ ім. Ігоря Сікорського, Україна

E-mail: ihor.berezovsky.24@gmail.com

Досліджені формати сигналів, що використовуються для створення радіоканалів в мережах мобільного зв'язку LTE. Розглянуто фізичний рівень радіоканалу: OFDM- мультиплексування з ортогональним частотним рознесенням на ділянці від базової станції до терміналу користувача, спектр і структурна схема формування OFDM-сигналів; SC-FDMA- мультиплексування з частотним рознесенням з передачею на одній несучій на ділянці від терміналу користувача до базової станції, структура сигналів і структура передачі даних технології SC-FDMA.

TECHNICAL PRINCIPLES OF SIGNAL TRANSMISSION IN LTE NETWORKS

Berezovskyi I.M.

Scientific adviser: **Noskov V.I.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: ihor.berezovsky.24@gmail.com

Investigated the signal formats, used to create radio channels in LTE mobile networks. The physical level of the radio channel is considered: OFDM multiplexing with orthogonal frequency diversity in the area from the base station to the user terminal, the spectrum and block diagram of the formation of OFDM signals; SC-FDMA multiplexing with frequency division and transmission on a single carrier in the area from the user terminal to the base station, the signal structure and the data transmission structure of the SC-FDMA technology.

ТЕХНІЧНІ ПРИНЦИПИ ТРАНСПОРТНИХ МЕРЕЖ MPLS TP

Маслак М.О.

Науковий керівник: **Носков В.І.**

Інститут телекомунікаційних систем

КПІ ім. Ігоря Сікорського, Україна

E-mail: misha.maslak384@gmail.com

Досліджено причини появи технології багатопроTOCOLьної комутації за мітками MPLS, основні принципи її роботи. Розглянуто історію створення пакетної транспортної мережі MPLS-TP, цілі її створення і основні вимоги до даної технології та її компонентів. Проведений аналіз основних відмінностей мережі MPLS-TP від MPLS.

TECHNICAL PRINCIPLES OF MPLS TP TRANSPORT NETWORKS

Maslak M.O.

Scientific adviser: **Noskov V. I.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: misha.maslak384@gmail.com

Investigated the emergence of Multiprotocol Label Switching (MPLS) technology and the basic principles of its operation. Considered the history of packet transport network MPLS-TP, its purpose and basic requirements to this technology and its components. Was carried out the analysis of main differences between MPLS-TP and MPLS networks.

ДОСЛІДЖЕННЯ ВИКОРИСТАННЯ ПРОТОКОЛІВ IPSEC ТА SSL В КОРПОРАТИВНІЙ МЕРЕЖІ

Корман Н.А. Науковий керівник: **Могилевич Д.І.**

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: kormannatasha21292@gmail.com

В роботі досліджено використання протоколів IPsec та SSL для підвищення рівня інформаційної безпеки в корпоративних мережах. На основі проведеного аналізу визначені основні переваги та недоліки цих протоколів, а також основні проблеми забезпечення інформаційної безпеки мережі при реалізації віртуальної мережі.

Домогтися високого ступеня захищеності інформації від несанкціонованого доступу в корпоративній мережі Інтернет є сумісне використання протоколів захищеної передачі даних: SSL (Secure Sockets Layer - рівень захищених сокетів); IPsec (IP Security - набір протоколів для забезпечення захисту даних, що передаються за допомогою протоколу IP).

На теперішній час протокол IPsec суттєво домінує і має ряд переваг у порівнянні від SSL: шифрування даних додаткового рівня, забезпечення безпеки маршрутизаторів, що надсилають дані про маршрутизацію через загальнодоступну мережу Інтернет; забезпечення аутентифікації без шифрування; захист мережевих даних, шляхом побудови схеми тунелю IPsec.

Предметом подальших досліджень є удосконалення методів побудови захищених з'єднань за допомогою протоколу IPSEC за схемами «точка-точка» і «мережа-мережа».

INVESTIGATION OF THE USE OF IPSEC AND SSL PROTOCOLS IN CORPORATE NETWORKS

Korman N.A. Scientific adviser: **Mogilevich D.I.**

Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute

E-mail: kormannatasha21292@gmail.com

The work is investigated of the use of IPsec and SSL protocols to increase the level of information security in corporate networks. Based on the analysis, the main advantages and disadvantages of these protocols, as well as the main problems of information security of the network in the implementation of the virtual network.

To achieve a high degree of protection of information from unauthorized access to the corporate Internet is the joint use of secure data transmission protocols: SSL (Secure Sockets Layer - level of secure sockets); IPsec (IP Security - a set of protocols to protect data transmitted using the IP protocol).

At present, the IPsec protocol significantly dominates and has a number of advantages over SSL: additional layer data encryption, security of routers that send routing data over the public Internet; providing authentication without encryption; protection of network data by building an IPsec tunnel scheme.

The subject of further research is to improve the methods of building secure connections using the IPSEC protocol on the schemes "point-to-point" and "network-network".

ТЕХНІЧНІ ПРИНЦИПИ ПОБУДОВИ ОПТИЧНИХ ТРАНСПОРТНИХ МЕРЕЖ

Бовсуновський Д.Р.

Науковий керівник: **Носков В. І.**

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: bovdem71@gmail.com

Досліджено історію розвитку оптичних транспортних мереж. Проаналізовані та порівняні між собою найбільш популярні технології оптичних транспортних мереж: DWDM та OTN-OTH.

TECHNICAL PRINCIPLES OF CONSTRUCTION OF OPTICAL TRANSPORT NETWORKS

Bovsunovskiy D. R.

Scientific adviser: **Noskov V. I.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: bovdem71@gmail.com

Investigated the history of optical transport networks development. Analyzed and compared the most popular technologies of optical transport networks: DWDM and OTN-OTH.

ПРОЕКТУВАННЯ ІЄРАРХІЧНИХ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ ДЛЯ МОНІТОРИНГУ ТРУБОПРОВODІВ

Москалюк С.О.

Науковий керівник: **Руренко О.Г.**

Інститут телекомунікаційних систем

КПІ ім. Ігоря Сікорського, Україна

E-mail: sviatoslav.moskaliuk@gmail.com

В роботі сформульовано підхід до створення ієрархічної бездротової сенсорної мережі для моніторингу трубопроводів. Проаналізовано стандарт передавання даних ZigBee та використання топології Mesh в розробці даної мережі.

DESIGN OF HIERARCHY WIRELESS SENSOR NETWORKS FOR PIPELINE MONITORING

Moskaliuk S.O.

Scientific adviser: **Rurenko O.G**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: sviatoslav.moskaliuk@gmail.com

An approach to creating a hierarchical wireless sensor network for monitoring pipelines is formulated. The ZigBee data transmission standard and the use of the Mesh topology in the development of this network are analyzed.

Засідання 2.

АНАЛІЗ ВРАЗЛИВОСТЕЙ МЕРЕЖІ ІОТ

Гіззатуллін Д. Д.

Науковий керівник: **Курдеча В. В**

Інститут телекомунікаційних систем,

КПІ ім. Ігоря Сікорського, Україна

E-mail: deny.gizz@gmail.com

По мірі того як користувацькі пристрої ІоТ стають все більш поширеними в нашому суспільстві, все більше закриваються вразливості, а також розробляються і вдосконалюються засоби захисту цих мереж. В даній роботі проаналізовано проблеми безпеки ІоТ. Результатом роботи є класифікація вразливостей мережі ІоТ у відповідності до семирівневої моделі мережі.

VULNERABILITY ANALYSIS OF IOT NETWORKS

Hizzatullin D. D.

Scientific adviser: **Kurdecha V.V.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: deny.gizz@gmail.com

As IoT devices become more widespread in our society, more and more diversity is being covered, as well as protection devices for these networks are being developed and improved. This work analyzes the security problems of the IoT. The result of the work is a classification of IoT network vulnerabilities according to the seven-layer network model.

МОДИФІКОВАНИЙ МЕТОД ВЗАЄМОДІЇ ВУЗЛІВ МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ

Карлін П.Ю.

Науковий керівник: **Курдеча В.В.**

Інститут телекомунікаційних систем

КПІ ім. Ігоря Сікорського, Україна

E-mail: kyiv12@bigmir.net

Робота присвячена розгляду варіативності взаємодії вузлів інтернету речей. Розглянуто типи та способи з'єднання вузлів інтернету речей. Досліджено особливості підключення вузлів ІОТ до мережі «Інтернет» та взаємодія пристроїв між собою. Проведено аналіз екосистеми та різновидів LPWAN мереж та мереж з невеликим діапазоном підключення, рівні та відповідні види протоколів. Ознайомлено з програмами штучного інтелекту, блокчейну, Kubernetes тощо.

MODIFIED METHOD OF IOT NODES INTERACTION

Karlin P.Y.

Scientific adviser: **Kurdecha V.V.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: kyiv12@bigmir.net

The work is devoted to the consideration of the variation of the interaction of the nodes of the Internet. Considered types and methods of connection of Internet nodes. Investigated features of connection of IOT nodes to the Internet and the interaction of devices between themselves. Analyzed of ecosystems and varieties of LPWAN networks and networks with a small range of, levels and types of protocols. Worked out applications of current technologies. Acquainted with programs of artificial intelligence, blockchain, Kubernetes, ETC.

АНАЛІЗ КОДУВАННЯ ДАНИХ В МЕРЕЖІ ІНЕТРНЕТУ РЕЧЕЙ

Ушаков С. М.

Науковий керівник: Курдеча В. В.

Інститут телекомунікаційних систем

КПІ ім. Ігоря Сікорського, Україна

E-mail: ushakovsergey21@gmail.com

З ростом актуальності і використання пристроїв IoT в сферах як інженерії та виробництва так і у повсякденному їх використанні, обсяги які передаються даних стрімко ростуть, а з ними ростуть рівні споживання трафіку та енергії. В роботі розглядаються методи кодування даних в мережі IoT, в результаті чого сформовано класифікацію наявних методів, визначені їх переваги та недоліки.

ANALYSIS OF IOT DATA ENCODING

Ushakov S. M.

Science adviser: **Kurdecha V. V.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: ushakovsergey21@gmail.com

With the growing relevance and use of IoT devices in the fields of engineering and manufacturing, as well as in their daily use, the volume of transmitted data is growing rapidly, and with them the levels of traffic and energy consumption. This paper examines methods of coding data in the IoT network, resulting in a classification of available methods, identifying their advantages and disadvantages.

УДОСКОНАЛЕНА АРХІТЕКТУРА ІОТ, ЗАСНОВАНА НА ТЕХНОЛОГІЯХ П'ЯТОГО ПОКОЛІННЯ

Березнюк А. В., Лазебний С.Г.

Науковий керівник: **Макаренко А.О.**

Державний університет телекомунікацій, Україна

E-mail: andrii.berezniuk@gmail.com

У дослідженні ми пропонуємо архітектуру ІоТ наступного покоління, засновану на технологіях 5G, яка відповідає вимогам майбутніх додатків та послуг. Ми порівнюємо різні архітектури, такі як SDN, QoS, SoA, S-IoT, IoT-A, для ефективного функціонування запропонованої нами архітектури. Крім того, ми розглядаємо методи збору та аналізу великих даних із сотень тисяч пристроїв від Smart City.

A NOVEL 5G BASED IOT ARCHITECTURE

Berezniuk A. V., Lazebnyi S. H.

Scientific adviser: **Makarenko A. O.**

State University of Telecommunications, Ukraine

E-mail: andrii.berezniuk@gmail.com

In our research, we suggest next-generation IoT architecture based on 5G technologies which meet the requirements of future applications and services. Particularly, we are comparing different architectures such as SDN, QoS, SoA, S-IoT, IoT-A with a modern one, suggested in this paper. Also we overview ways of Big Data analysis and collection from hundreds of thousands of devices from Smart City.

ПРОБЛЕМИ ЗАХИСТУ ДАНИХ В МЕРЕЖІ 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 проблемам захисту даних в мережі Інтернету речей. Розглянуто безпосередньо поняття безпеки в IoT. Досліджено структурну модель мережі Інтернету речей і перераховано основні технології, які використовуються в IoT. Проаналізовано недоліки і вразливості, відповідно до розглянутих структурних складових і методів. Доведено ефективність використання нових підходів для забезпечення інформаційної безпеки.

DATA PROTECTION VULNERABILITIES IN THE INTERNET OF THINGS

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 the problems of data protection in the Internet of Things. Considered the directly concept of security in IoT. Studied the structural model of the Internet of Things and listed the main technologies used in IoT. Analyzed disadvantages and vulnerabilities in accordance with the considered structural components and methods. Delivered the efficiency of using new forecasts for providing information security.

ОРГАНІЗАЦІЯ ПРОТИДІЇ ЗАГРОЗАМ ПОРУШЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Тимофєєв Є.М.

Науковий консультант: **Созонник Г.Д.**

Інститут телекомунікаційних систем

КПІ ім. Ігоря Сікорського, Україна

E-mail: timofeevzh@gmail.com

Здійснено аналіз сучасних технологій щодо надання безпеки сервісу побудови віртуальних приватних мереж, технічних рішень технології VPN на прикладі організації приватної віртуальної мережі на основі мережі MPLS. Встановлено причини необхідності захисту від атак. Запропонована методика комплексного захисту даних підприємства при організації сервісу безпеки VPN.

ORGANIZATION FOR COUNTERING INFORMATION SECURITY THREATS

Tymofeiev Y.M.

Scientific consultant: **Sozonnyk H.D.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: timofeevzh@gmail.com

Modern technologies for providing security of the service of building virtual private networks, technical solutions of VPN technologies on the example of the organization of a private virtual network based on MPLS network are analyzed. The reasons for the need to protect against attacks are identified. The technique of complex data protection of the enterprise at the organization of VPN security service is offered.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ЗАСОБІВ ШТУЧНОГО ІНТЕЛЕКТУ В ТЕХНОЛОГІЇ SECURE SD-WAN

Персіков М.А.¹, Лемешко В.О.²

Науковий керівник: **Єременко О.С.²**

¹*Харківський патентно-комп'ютерний коледж,*

²*Харківський національний університет радіоелектроніки, Україна*

E-mail: mihapersikov@gmail.com, valentyn.lemeshko@nure.ua

З урахуванням потенційних уразливостей з боку інформаційної безпеки проаналізовано особливості додаткового використання засобів штучного інтелекту в межах територіально розподілених транспортних мереж, а саме Secure SD-WAN. Використання цієї технології дозволяє забезпечити достатній рівень якості сприйняття (Quality of experience, QoE), доступ до сегментів мережі, інтегровану безпеку, захист мультихмари, глибоку видимість мережі, моніторинг уразливостей окремих її ділянок та ін. Виявлено, що завдяки використанню засобів штучного інтелекту в процесі управління трафіком підвищується рівень безпеки та відмовостійкості завдяки переходу від реактивних до проактивних мережних рішень.

FEATURES OF ARTIFICIAL INTELLIGENCE APPLICATION IN SECURE SD-WAN TECHNOLOGY

Persikov M.A.¹, Lemeshko V.O.²

Scientific adviser: **Yeremenko O.S.²**

¹*Kharkiv Patent and Computer College,*

²*Kharkiv National University of Radio Electronics, Ukraine*

E-mail: mihapersikov@gmail.com, valentyn.lemeshko@nure.ua

Considering potential vulnerabilities in the field of information security, the features of additional use of artificial intelligence within the transport networks, namely Secure SD-WAN, have been analyzed. The application of this technology allows ensuring a sufficient level of perception quality (Quality of Experience, QoE), access to network segments, integrated security, multi-cloud protection, deep network visibility, threats monitoring in some parts of it, etc. It was found that the use of artificial intelligence in the process of traffic management increases the level of security and fault-tolerance due to the transition from reactive to proactive network solutions.

УДОСКОНАЛЕНА МЕТОДИКА ОЦІНКИ СТРУКТУРНОЇ НАДІЙНОСТІ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ ЗВ'ЯЗКУ

Папушой О.К.

*Науковий керівник: Могилевич Д.І.
Інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: o.papushoyyy@gmail.com*

На основі запропонованої удосконаленої методики проведено оцінку залежності показників структурної надійності інформаційних напрямків від структури цих напрямків (довжина та кількість шляхів які входять до інформаційного напрямку). Аналіз отриманих результатів показав, що залежність показників структурної надійності інформаційних напрямків від структури (загальної топології) цих напрямків має монотонний характер без перегинів. Також простежується вплив на показники структурної надійності значення рангу комунікаційних центрів.

IMPROVED METHODOLOGY OF ESTIMATION OF STRUCTURAL RELIABILITY OF MULTISERVICE COMMUNICATION NETWORK

Papushoi O.K.

*Scientific adviser: Mogilevich D.I.
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: o.papushoyyy@gmail.com*

On the basis of the offered improved technique the estimation of dependence of indicators of structural reliability of information directions on structure of these directions is carried (length and amount of ways included in the information direction). The analysis of the obtained results showed that the dependence of the indicators of structural reliability of information directions on the structure (general topology) of these directions has a monotonous character without kinking. The influence of value of the rank of communication centers on the indicators of structural reliability is also traced.

ПОТОКОВА МОДЕЛЬ БАЛАНСУВАННЯ НАВАНТАЖЕННЯ В ІНФОКОМУНІКАЦІЙНІЙ МЕРЕЖІ

Круглова А.О., Журавльова А.С.

Науковий керівник: Лемешко О.В.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського

Харківський національний університет радіоелектроніки

E-mail: anastasiia.kruhlova@nure.ua, anna.zhuravlova@nure.ua

У даній роботі запропоновано вдосконалену математичну модель балансування навантаження в інфокомунікаційній мережі, що відповідає принципам концепції Traffic Engineering. Для підвищення відмовостійкості в даній моделі, кожна мережа доступу підключена одночасно не до одного, а до декількох приграничних маршрутизаторів. Для покращення рівня балансування навантаження в інфокомунікаційній мережі, пропонується розподілити трафік на рівні доступу між декількома приграничними маршрутизаторами, що створюють віртуальний шлюз за замовчуванням. Забезпечення балансування навантаження дозволило підвищити продуктивність мережі та знизити верхній поріг використання каналів зв'язку.

FLOW-BASED MODEL OF LOAD BALANCING IN THE INFOCOMMUNICATION NETWORK

Kruhlova A.O., Zhuravlova A.S.

Scientific adviser: Lemeshko O.V.

Department of Infocommunication Engineering V.V. Popovsky

Kharkiv National University of Radioelectronics

E-mail: anastasiia.kruhlova@nure.ua, anna.zhuravlova@nure.ua

This paper proposes an improved mathematical model of load balancing in the network infocommunication system, which corresponds to the principles of the concept of Traffic Engineering. To increase fault tolerance in this model, each access network is connected simultaneously to not one, but to several border routers. To improve the level of load balancing in the infocommunications network, it is proposed to distribute traffic at the access level between several border routers, creating a default virtual gateway. Ensuring load balancing has increased network performance and lowered the upper threshold for communication channels.

РЕАЛІЗАЦІЯ МЕРЕЖІ І ДІЯЛЬНОСТІ СУЧАСНОЇ КОМПАНІЇ НА ОСНОВІ ПРОДУКТІВ MICROSOFT

Бузян С.О.

Науковий керівник: **Григоренко О.Г.**

Інститут телекомунікаційних систем

КПІ ім. Ігоря Сікорського, Україна

E-mail: svyatik007@gmail.com

Розглянуті можливості забезпечення ефективної діяльності сучасної компанії на основі продуктів Microsoft. Особлива увага приділена прикладам побудови мережі, що забезпечують функціонування застосунків та програмного забезпечення Microsoft.

THE MODERN COMPANY'S NETWORK AND ACTIVITIES IMPLEMENTATION BASED ON MICROSOFT

Buzyan S.O.

Scientific adviser: **Grygorenko O.G.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: svyatik007@gmail.com

Possibilities of ensuring the effective operation of a modern company on Microsoft products are considered. Particular attention is paid to the example of a network design that ensures the operation of Microsoft applications and software.

АНАЛІЗ ВИКОРИСТАННЯ СУПУТНИКІВ НИЗЬКОЇ НАВКОЛОЗЕМНОЇ ОРБИТИ ДЛЯ ВИРІШЕННЯ ЗАДАЧ ВСЕСВІТНЬОЇ МЕРЕЖЕВОЇ ВЗАЄМОДІЇ

Биков П.І.

Науковий керівник: **Кононова І.В.**

Інститут телекомунікаційних систем

КПІ ім. Ігоря Сікорського, Україна

E-mail: pavlouk2012@gmail.com

Досліджено принципи роботи існуючих та перспективних супутникових систем низької навіколоземної орбіти для введення їх в експлуатацію. В роботі проаналізовано перспективи використання високошвидкісних супутникових ліній зв'язку, їх конкурентні переваги у порівнянні з існуючими каналами передачі даних.

Розглянуто кон'юнктуру ринку телекомунікацій в Україні, враховуючи зростаючий попит на супутникові канали зв'язку, а також проведено дослідження щодо організації розгортання супутникового зв'язку з лінією прив'язки до стаціонарної транспортної телекомунікаційної мережі.

ANALYSIS OF THE USE OF LOW EARTH ORBIT SATELLITES TO SOLVE THE PROBLEMS OF GLOBAL NETWORK INTERACTION

Bykov P.I.

Scientific adviser: **Kononova I.V.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: pavlouk2012@gmail.com

Researched operation principles of existing and planned low-Earth orbit satellite systems for their commissioning. The article analyzes the prospects of using high-speed satellite communication lines, their competitive advantages compared to existing data transmission channels.

The situation of the telecommunications market in Ukraine is considered, taking into account the growing demand for satellite communication channels, as well as a study on organization of deployment satellite communication with a line of connection to a stationary transport telecommunication network.

ПОБУДОВА ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ НА ОСНОВІ ТЕХНОЛОГІЇ MPLS

Цимбал Г.О.

Науковий керівник: **Григоренко О.Г.**

Інститут телекомунікаційних систем

КПІ ім. Ігоря Сікорського, Україна

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

Розглянуто призначення та переваги застосування технології віртуальних приватних мереж (VPN). Проаналізовано особливості побудови VPN на базі технології MPLS. Зазначена актуальність VPN для забезпечення конфіденційності і цілісності даних.

DESIGN OF VIRTUAL PRIVATE NETWORKS BASED ON MPLS TECHNOLOGY

Tsymbal G.O.

Scientific adviser: **Grygorenko O.G.**

Institute of Telecommunication Systems,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

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

The purpose and advantages of using virtual private network (VPN) technology are discussed. Features of VPN design based on MPLS technology are analyzed. It is noted that VPN is relevant to ensure the data confidentiality and integrity.