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

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ НДІ ТЕЛЕКОМУНІКАЦІЙ

Сімнадцята міжнародна науково-технічна конференція "ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ"
і
П'ятнадцята міжнародна науково-технічна конференція студентів та аспірантів «ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА СИСТЕМ»

Конференцію присвячено:
125-річчю Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»
20-річчю Навчально-наукового інституту телекомунікаційних систем
30-річчю кафедри Телекомунікацій

18–21 квітня 2023 року

Матеріали конференції

м. Київ

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

EDUCATIONAL AND RESEARCH INSTITUTE
OF TELECOMMUNICATION SYSTEMS
RESEARCH INSTITUTE OF TELECOMMUNICATIONS

Seventeenth International Scientific Conference
"MODERN CHALLENGES IN TELECOMMUNICATIONS"

and

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

The conference is dedicated:
125th anniversary of the National Technical University of Ukraine "Ihor Sikorsky Kyiv Polytechnic Institute"
20th anniversary of the Educational and Scientific Institute of Telecommunication Systems
30th anniversary of the Department of Telecommunications

April 18-21, 2023

Conference proceedings

Kyiv

ISSN (print) 2663-502X
ISSN (online) 2664-3057

XVII Міжнародна науково-технічна конференція "Перспективи телекомунікацій" ПТ-2023: Збірник матеріалів конференції. К.: КПІ ім. Ігоря Сікорського, 2023. – с.385.

XVII International Scientific Conference "Modern Challenges in Telecommunications" MCT-2023. Conference proceedings. Kyiv. Igor Sikorsky Kyiv Polytechnic Institute, 2023 – p. .385.

XV Міжнародна науково-технічна конференція студентів та аспірантів «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем» ПРІТС 2023: Збірник тез конференції. К.: КПІ ім. Ігоря Сікорського, 2023.

Збірник містить матеріали пленарних і секційних доповідей, представлених на Сімнадцятій міжнародній науково-технічній конференції "Перспективи телекомунікацій" (ПТ 2023) та П’ятнадцятій міжнародній науково-технічній конференції студентів та аспірантів «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем» (ПРІТС 2022), дати проведення 18–21 квітня 2023 р. в м. Києві.

Електрона 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.uran.ua/ (ISSNonline 2664-305).

Робочими мовами конференцій є українська та англійська.

У збірник включені матеріали конференції за такими секціями:

1. Достовірність та ефективність передачі інформації.
2. Мережні, оптоволоконні технології та безпека.
3. Безпроводові технології, системи мобільного зв’язку.
4. Інформаційні технології в телекомунікацій.
5. Сенсорні мережі та Інтернет речей.

Секретар оргкомітету конференції *Іванова Т.Л.*
t.me/MNTK_PT;. *E-mail: conf@its.kpi.ua*

Співголови конференції "Перспективи телекомунікацій":

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

БАРАНОВ О.А. – керівник Наукового центру цифрової трансформації і права Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України», д.ю.н., професор.

Організатори конференції:

Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», НН ІТС, НДІ телекомунікацій;
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 НН ІТС, а також всі бажаючі.

Координатор Програмного комітету:

КРАВЧУК С.О. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ.
НОВОГРУДСЬКА Р.Л.- к.т.н., доц., КПІ ім. Ігоря Сікорського, (П, 6), 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;
ЛАВРУТ О.О. - д.т.н., проф., НАСВ ім. гетьмана Петра Сагайдачного, (3), Львів;
ЛЕМЕШКО О.В. - д.т.н., проф., ХНУРЕ, Харків;
ЛИСЕНКО О.І. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;

ЛУНТОВСЬКИЙ А.О. - Prof. at BA Dresden University, Дрезден, Німеччина;
МАКСИМОВ В.В. - к.т.н., доц. КПІ ім. Ігоря Сікорського, Київ;
МІНОЧКІН Д.А. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
МОШИНСЬКА А.В. - д.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
НАЗАРЕНКО О.І. – факультет лінгвістики КПІ ім. Ігоря Сікорського, м. Київ;
НАРИТНИК Т.М. - к.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
ПОПОВ В.І. - д.м.-ф.н., проф., РТУ, м. Рига, Латвія;
ПРАВИЛО В.В. – к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
РОМАНОВ О.І. - д.т.н., проф., КПІ ім. Ігоря Сікорського, Київ;
РОМАНЮК В.А. - д.т.н., проф. ВІТІ, Київ;
СЕРГІЄНКО М.І. – ст. викладач каф. ІЕ, ІЕЕ, КПІ ім. Ігоря Сікорського, Київ;
СКУЛИШ М.А. - д.т.н., с.н.с., КПІ ім. Ігоря Сікорського, Київ;
СТРИЖАК О.Є. - к.т.н., НЦ «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;
ЧУМАЧЕНКО С.М. - д.т.н., с.н.с., НУХТ, Київ;
ШПІЛЬНЕР Йозеф - Dr. at ZHAW School of Engineering, Цюріх, 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:

Дуля Ю.А. – головний бухгалтер НДІ ТК.
Березовська О.В. – реєстрація, забезпечення документообігу.
Мікляєв О.В. – технічне обслуговування.
Іванова Т.Л. – оформлення конференції на сайті НН ІТС.
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., t.me/MNTK_PT,, conf@its.kpi.ua.

Адреса проведення конференції:

Конференцію було проведено у змішаному форматі: очно (корпус № 6 зал засідань, м. Київ, пр. Перемоги, 37-е) та дистанційно (за допомогою on-line сервісів для відеоконференцій та вебінарів ZOOM).

ЗМІСТ

Пленарні доповіді

Доповідачі:

Ільченко М.Ю., Кравчук С.О., Уривський Л.О.
ПРОДОВЖЕННЯ СПРАВИ АКАДЕМІКА ГЛУШКОВА В.М. У РОЗВИТКУ СУЧАСНИХ ІНФО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ.....19

Кононова І.В.
1000+ НОВИНИ ІНФОТЕЛЕКОМУ 25

Victor Suzdal, Ihor Tavrovsky
SCINTILLATION DETECTORS BASED ON NaI:Tl WITH 3% RESOLUTION IN CLASSIFICATION TASKS USING NEURAL NETWORKS 30

Правило В.В.
АНАЛІЗ ПОТЕНЦІЙНИХ ВРАЗЛИВОСТЕЙ ТА ЗАГРОЗ В 5G 33

Сушин І.О., Лисенко О.І.
ПРОГРАМА ОЦІНКИ ЗВ'ЯЗНОСТІ ВУЗЛІВ БЕЗПРОВОДОВИХ ЕПІЗОДИЧНИХ МЕРЕЖ ПРИ УМОВІ ЗАСТОСУВАННЯ БПЛА 36

Жабчик А.І., Нарушкевич О.М., Наритник Т.М., Капштик С.В.
ПРОГРАМНО-КОНФІГУРОВАНА СУПУТНИКОВА ІНФРАСТРУКТУРА ІНТЕРНЕТУ РЕЧЕЙ.....42

Ільченко М.Ю., Якорнов Є.А.
ВПРОВАДЖЕННЯ ЗАГАЛЬНИХ ПРИНЦИПІВ «STEM-ОСВІТИ» В НАВЧАЛЬНО-НАУКОВОМУ ІНСТИТУТІ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ КПІ ІМ. ІГОРЯ СІКОРСЬКОГО.....47

Лісовський К.С., Буглак А.О.
НАУКОВА ДІЯЛЬНІСТЬ СТУДЕНТІВ НАВЧАЛЬНО-НАУКОВОГО ІНСТИТУТУ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ КПІ ІМ. ІГОРЯ СІКОРСЬКОГО 54

Секція 1. Достовірність та ефективність передачі інформації

Співголови:

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

Доповідачі:

Лівенців С.П.
ЗАСТОСУВАННЯ ГЕНЕТИЧНОГО АЛГОРИТМУ ДЛЯ СИНТЕЗУ ОПТИМАЛЬНОЇ СТРУКТУРИ ТУРБОКОДУ 59

Максимов В.В., Носков В.І., Храповицький І.А.
НОВІ КОМПОЗИТНІ ПОСЛІДОВНОСТІ БАРКЕРА В СИСТЕМАХ З ПРЯМИМ РОЗШИРЕННЯМ СПЕКТРУ 62

Тихонов М.В.
УДОСКОНАЛЕНИЙ МЕТОД ПОБУДОВИ МОДЕЛЕЙ ОЦІНКИ НАДІЙНОСТІ ОБ'ЄКТІВ ЕЛЕКТРОННОГО КОМУНІКАЦІЙНОГО ОБЛАДНАННЯ З КОМБІНОВАНИМ РЕЗЕРВОМ ЧАСУ 65

Уривський Л.О., Сколець А.В.
ДОСЛІДЖЕННЯ ВПЛИВУ ФАКТОРУ САМОПОДІБНОСТІ НА ФУНКЦІОНУВАННЯ СМО 68

Носков В.І.
ОЦІНКА ПОТЕНЦІЙНИХ МОЖЛИВОСТЕЙ РАДІОКАНАЛІВ МОБІЛЬНИХ МЕРЕЖ 5G 72

Бердников О.М.
СТРУКТУРИ ОПТИЧНИХ СЕКЦІЙ ЛІНІЙНИХ ТРАКТІВ ВОСП СУ ІЗ ГРАНИЧНО МІНІМАЛЬНИМ OSNR 75

Голяткін А. О., Мошинська А. В.
РОЗШИРЕННЯ ФУНКЦІОНАЛУ ПРИСТРОЇВ TUYA SMART З ВИКОРИСТАННЯМ МОВИ ПРОГРАМУВАННЯ PYTHON 78

Кононова І.В. , Самусь Д.В., Самусь Г.І.
АНАЛІЗ ПРОБЛЕМ ПРИ РЕАЛІЗАЦІЇ ТЕХНОЛОГІЇ ІНДУСТРІАЛЬНОГО ІНТЕРНЕТА РЕЧЕЙ 81

Бабич І.О., Осипчук С.О.
ДОСЛІДЖЕННЯ IOT M2M-ПРОТОКОЛІВ ДЛЯ ЗНИЖЕННЯ ЙМОВІРНОСТІ ДТП 84

Григоренко О.Г., Реута Г.В.
ВИКОРИСТАННЯ ЦИФРОВИХ ПІДПИСІВ І СЕРТИФІКАТІВ ДЛЯ БЕЗПЕКИ ТРАНЗАКЦІЙ І ПІДТВЕРДЖЕННЯ СПРАВЖНОСТІ ЕЛЕКТРОННИХ ДОКУМЕНТІВ 87

Григоренко О.Г., Голуб О.С.
КОНФІДЕНЦІЙНІСТЬ ДАНИХ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ І ЗАСОБИ ЇЇ ЗАБЕЗПЕЧЕННЯ 90

Секція 2. Мережні, оптоволоконні технології та безпека

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

Доповідачі:

Triska N.R.
PERSPECTIVE TRENDS OF TELECOMMUNICATION NETWORKS DEVELOPMENT BASED ON IMT-2030 CONCEPT 93

Trubarov I.V.
PRINTED DIPOLE ANTENNA FOR 2.4 GHZ FREQUENCY BAND 96

Trubarov I.V.
MICROSTRIP RING ANTENNA FOR 2.4 GHZ FREQUENCY BAND 99

Романов О.І., Сколець С.С., Марінов А.І.
МОДЕЛЮВАННЯ МЕРЕЖІ SDN З ВИКОРИСТАННЯМ ВІДКРИТОЇ МЕРЕЖЕВОЇ ОПЕРАЦІЙНОЇ СИСТЕМИ ONOS 102

Верес Л.А.
ІНТЕГРАЦІЯ АРХІТЕКТУРИ ПРОТОКОЛІВ IMS В МЕРЕЖІ 5G 106

Маньківський В.Б., Конахович Г.Ф., Романов А.О.
ДОДАТКОВИЙ МЕХАНІЗМ МЕРЕЖЕВОЇ ВЗАЄМОДІЇ IN KUBERNETES 109

Іванов С.В., Олійник П.Б., Вірченко Г.А.
НАМОТОЧНА МАШИНА ДЛЯ ВИГОТОВЛЕННЯ КОТУШОК ВОЛОКОННО-ОПТИЧНИХ ГІРОСКОПІВ 112

Бурлака Г.Ю.
УПРАВЛІННЯ МЕРЕЖЕЮ SDN З ВИКОРИСТАННЯМ КОНТРОЛЕРА Ryu 116

Чумаченко К.Д., Романов О.І.
ВИКОРИСТАННЯ LI-FI В МЕДИЦИНІ 119

Підпалий О.І.
ЯКІСТЬ ОБСЛУГОВУВАННЯ НА ОСНОВІ SIP 122

Берестовенко О.О., Маньківський В.Б.
ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРОДУКТИВНОСТІ СУЧАСНИХ ПРОГРАМНИХ КОМУТАТОРІВ 126

Маньківський В.Б., Мінжинер Н.М.
ПЕРЕВАГИ ПРОГРАМНОГО КОМПЛЕКСУ З АРХІТЕКТУРНИМ ПАТТЕРНОМ SIDE-EFFECT З ISTIO 130

Романов О.І., Сколець С.С., Марінов А.І.
РОЗГОРТАННЯ ONOS КЛАСТЕРУ ДЛЯ ЕМУЛЯЦІЇ РОБОТИ КОРИСТУВАЦЬКОЇ МЕРЕЖІ SDN 133

Сколець С.С., Марінов А.І., Нестеренко М.М.
ОСОБЛИВОСТІ ПОБУДОВИ РОЗПОДІЛЕНОЇ МЕРЕЖЕВОЇ ОПЕРАЦІЙНОЇ СИСТЕМИ ONOS 137

Сайченко І.О.
МОДЕЛЮВАННЯ МЕРЕЖІ SDN НА СТОРОНІ КІНЦЕВОГО КОРИСТУВАЧА 141

Дрьомова А.О., Авдєєнко Г.Л.
АПАРАТНО-ПРОГРАМНИЙ КОМПЛЕКС ДЛЯ ДОСЛІДЖЕННЯ ПАРАМЕТРІВ СИГНАЛІВ СУПУТНИКОВОГО ТЕЛЕВІЗІЙНОГО МОВЛЕННЯ 145

Поливана В.В., Романов М. О.
ПОБУДОВА МЕРЕЖІ ШИРОКОСМУГОВОГО ДОСТУПУ З ПІДТРИМКОЮ SDN НА БАЗІ ПЛАТФОРМИ SEBA 148

Trubin A. A.
ON ONE POSSIBILITY OF CONSTRUCTING BAND-PASS FILTERS BASED ON OPTICAL MICRO-RESONATORS WITH WHISPERING GALLERY OSCILLATIONS 155

Trubin A. A.
SCATTERING OF PLANE WAVES ON ONE-DIMENSIONAL LATTICES OF SPHERICAL DIELECTRIC RESONATORS 155

Секція 3. Безпроводові технології, системи мобільного зв'язку

Співголови:

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

Доповідачі:

Oliinyk D.I., Nizhnyi D.A.
BROADBAND WIRELESS COMMUNICATION IN THE TERAHERTZ RANGE: THE KEY TO THE SUSTAINABILITY OF THE DIGITAL ECONOMY 159

Черняк А.М., Наритник Т.М., Шевченко Т.А.
ОСОБЛИВОСТІ І ТЕНДЕНЦІЇ ТРОПОСФЕРНИХ СИСТЕМ ЗВ'ЯЗКУ ..162

Ніконенко В.О., Авдєєнко Г.Л.
РОЗРОБЛЕННЯ МАКЕТУ ДЛЯ ДОСЛІДЖЕННЯ ПРИЙМАЧІВ СИСТЕМ СУПУТНИКОВОЇ РАДІОНАВІГАЦІЇ.....165

Василенко С. В., Єрохін В. Ф., Зінченко Я. В.
АНАЛІЗ ЗАВАДОСТІЙКОСТІ АЛГОРИТМУ ВХОДЖЕННЯ В СИНХРОНІЗМ РАДІОЛІНІЇ З ППРЧ НА ОСНОВІ ОЦІНКИ ФАЗИ М-ПОСЛІДОВНОСТІ 168

Кисіль А. В., Авдєєнко Г. Л.
ОГЛЯД СУЧАСНИХ ТЕХНОЛОГІЙ ЦИФРОВОГО ТЕЛЕВІЗІЙНОГО МОВЛЕННЯ 171

Гуйда О.Г., Омецинська Н.В., Новіков В.І., Гетьман О.В.
ПРОБЛЕМИ ПРОЕКТУВАННЯ АРХІТЕКТУРИ БЕЗДРОТОВОЇ СЕНСОРНОЇ МЕРЕЖІ 174

Тачиніна О.М., Гуйда О.Г., Явіся В.С., Гетьман О.В.
МЕТОДИ ЕНЕРГОЗБЕРЕЖЕННЯ НА ОСНОВІ ЕНЕРГОЕФЕКТИВНОЇ КЛАСТЕРИЗАЦІЇ ДЛЯ WSN.....177

Правило В.В.
АНАЛІЗ НАПРЯМКІВ ПОБУДОВИ РАЦІОНАЛЬНОЇ АРХІТЕКТУРИ МЕРЕЖІ 5G НА ОСНОВІ ІСНУЮЧИХ 4G МЕРЕЖ 180

Гетьман О.В., Кайденко М.М., Роскошний Д.В.
ВИКОРИСТАННЯ ТЕХНОЛОГІЇ МРТСР ДЛЯ ПІДВИЩЕННЯ ЖИВУЧОСТІ WIFI КАНАЛІВ УПРАВЛІННЯ БПЛА В УМОВАХ ВПЛИВУ НАВМИСНИХ ТА НЕНАВМИСНИХ ЗАВАД 183

Гетьман О.В., Кайденко М.М., Роскошний Д.В.
ВИКОРИСТАННЯ СИСТЕМ-НА-КРИСТАЛІ РАДІОЧАСТОТНОГО ЗАСТОСУВАННЯ ПРИ РОЗРОБЦІ SDR СИСТЕМ 186

Кравчук С.О.
ВІДКРИТА АРХІТЕКТУРА DRONE ID ТА ПРОТОКОЛ ДИСТАНЦІЙНОЇ ІДЕНТИФІКАЦІЇ ДРОНІВ.....189

Кравчук С.О., Кравчук І.М.
ТЕХНОЛОГІЇ ТА СИСТЕМИ ПРОТИДІЇ ЗАГРОЗАМ ВІД МАЛИХ ДРОНІВ 192

Кравчук С.О., Чуб М.М.
РЕЗУЛЬТАТИ АНАЛІЗУ ТЕРМІНОЛОГІЇ В ГАЛУЗІ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ ІЗ ЗАСТОСУВАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ 195

Явіся В.С., Лисенко О.І., Гетьман О.В.
СПОСІБ ПІДВИЩЕННЯ КОЕФІЦІЄНТА ПОСИЛЕННЯ ПРИЙМАЛЬНО-ПЕРЕДАВАЛЬНОГО ОБЛАДНАННЯ КАНАЛУ ЗВ’ЯЗКУ З ДРОНАМИ 198

Міночкін Д.А., Мацюк Е.О.
СИСТЕМА ІНТЕРНЕТУ РЕЧЕЙ НА БАЗІ МЕРЕЖІ 5G 201

Ветошко І.П.
ОЦІНКА НАУКОВОГО НАПРЯМУ ДОСЛІДЖЕНЬ ГОЛОСОВИХ ПОСЛУГ У МЕРЕЖАХ 5-ГО ПОКОЛІННЯ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ CHATGPT.....205

Карпишин Н.Я., Кравчук С.О.
ДОСЛІДЖЕННЯ МЕТОДІВ МОНІТОРИНГУ ТРАФІКУ ДЛЯ ПРОТИДІЇ ФРОДУ В IP-ТЕЛЕФОНІЇ 208

Мєщерінов М.В.
ВИКОРИСТАННЯ CHAT GPT ДЛЯ ВИЗНАЧЕННЯ ПРОБЛЕМИ ПЕРЕДАЧІ ВІДЕО СИГНАЛУ ЧЕРЕЗ ПРИСТРОЇ IOT 211

Остапов О.А., Чуб М.М., Афанасьєва Л.О.
СКЛАДНОЩІ НАСКРІЗНОГО E2E ТЕСТУВАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ 214

Міночкін Д. А., Кошмак А.І.
ПОРІВНЯННЯ ТРАДИЦІЙНОЇ МОДЕЛІ ВИЯВЛЕННЯ ШАХРАЙСТВА, З МАШИННИМ НАВЧАННЯМ.....217

Руренко О.Г., Денищич Н.М.
ВИКОРИСТАННЯ ПРОТОКОЛУ ZIGBEE В БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖАХ: РОЗРОБКА JAVA ДОДАТКУ ДЛЯ МОНІТОРИНГУ ПРИСТРОЇВ НА ОСНОВІ ZIGBEE 220

Секція 4. Інформаційні технології в телекомунікаціях

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

Доповідачі:

Глоба Л.С., Новогрудська Р.Л., Копійка О.В.
ОНТОЛОГІЧНЕ МОДЕЛЮВАННЯ ТЕХНОЛОГІЧНИХ ПРОЦЕСІВ ДЛЯ ВИРОБНИЦТВА ДЕТАЛЕЙ СКЛАДНОЇ ФОРМИ 223

Пархоменко Д.О., Скулиш М.А.
РОЗРОБКА МЕТОДУ ДИНАМІЧНОГО КЕРУВАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЮ ІНФРАСТРУКТУРОЮ 226

Forostianko K.Y., AstrakhantsevA.A.
EFFICIENCY OF USER AUTHENTICATION METHODS IN MOBILE NETWORKS 229

Sushko O.V., Astrakhantsev A.A.
STUDY OF THE EFFICIENCY OF MACHINE LEARNING ALGORITHMS FOR TRAFFIC CLASSIFICATION IN MOBILE NETWORKS 232

Вигівський М.С., Денисенко М.С., Капштик С.В., Наритник Т.М.
ОРГАНІЗАЦІЯ УПРАВЛІННЯ НАВКОЛОМІСЯЧНИМ УГРУПОВАННЯМ КУБСАТ (CUBESAT) ЗА ДОПОМОГОЮ МІСЯЧНОГО ПОСАДКОВОГО МОДУЛЯ 235

Дмитренко О.А.
МІКРОСЕРВІСНА АРХІТЕКТУРА ТА ЇЇ ЗАДАЧІ НА ПРИКЛАДАХ З РЕАЛЬНОГО ЖИТТЯ 239

Омельченко С.А., Маньківський В.Б.
МЕТОД ПОБУДОВИ ЗАВАДОСТІЙКОГО ПРОГРАМНОГО КОМПЛЕКСУ З ВИКОРИСТАННЯМ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ 243

Єрмолаєв О. Д., Суліма С.В.
ОПТИМІЗАЦІЯ ВИКОНАННЯ ЗАПИТІВ У РЕЛЯЦІЙНІЙ СИСТЕМІ УПРАВЛІННЯ БАЗАМИ ДАНИХ 246

Глоба Л.С., Райчук А.А., Прокопець Н.А.
КОМПЛЕКСНИЙ МЕТОД ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ОБРОБКИ НАВАНТАЖЕННЯ У РОЗПОДІЛЕНИХ ЦОД ОПЕРАТОРІВ ЗВ'ЯЗКУ 249

Смаглюк В.О., Алєксєєв М.О.
КЕРУВАННЯ ОБЧИСЛЮВАЛЬНИМИ РЕСУРСАМИ КОРИСТУВАЦЬКИХ ПРИСТРОЇВ У СКЛАДІ КЛАСТЕРУ KUBERNETES 253

Кудляк В.М., Бєлан Т.І., Новогрудська Р.Л.
ТРАНСДИСЦІПЛІНАРНИЙ ПІДХІД ДО ВИСВІТЛЕННЯ МУЗЕЙНИХ АРТЕФАКТІВ НА БАЗІ ОНТОЛОГІЙ.....257

Приходнюк В. В., Горборуков В. В.
ОНТОЛОГОКЕРОВАНІ КОГНІТИВНІ СЕРВІСИ ЯК СКЛАДОВА ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ АНАЛІЗУ СТАТИСТИЧНОЇ ІНФОРМАЦІЇ 260

Курдеча В.В., Любарска С.І.
АНАЛІЗ ТА ПОРІВНЯННЯ МЕТОДІВ ОБРОБКИ ГРАФІЧНОЇ ІНФОРМАЦІЇ В МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ 263

Бушинський Д.А., Курдеча В.В.
ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖІ ІНТЕРНЕТ РЕЧЕЙ...266

Корнійчук І. Г., Курдеча В.В.
ЕНЕРГЕТИЧНЕ ПРОГНОЗУВАННЯ ТА УПРАВЛІННЯ З ПІДТРИМКОЮ ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ ГІБРИДНИХ МІКРОМЕРЕЖ 269

Ковальська Д.Д., Курдеча В.В.
ПРОБЛЕМИ АУДИТУ ІНФОКОМУНІКАЦІЙНОЇ МЕРЕЖІ ВЕЛИКИХ ПІДПРИЄМСТВ.....272

Вішталь Д.М., Любашенко Н.Д.
СИСТЕМА МОДЕЛЮВАННЯ ДОСТУПНОСТІ МЕРЕЖЕВИХ ПОСЛУГ.....275

Бугайов М.В.
ДЕТЕКТОР СТОХАСТИЧНИХ СИГНАЛІВ.....278

Секція 5. Сенсорні мережі та Інтернет речей

Співголови:

д.т.н., проф. Лисенко О.І., д.т.н., проф. Романюк В.А., д.т.н., проф. Жук С.Я.

Доповідачі:

Kamarali R.., Krylach O., Zhivkov A., Shevtsov K., Stepanenko V.M.
MICROWAVE DIRECTIONAL FILTERS.....281

Цуканов С.О., Глоба Л. С.
ЗАСТОСУВАННЯ МЕТОДІВ НЕЧІТКОЇ ЛОГІКИ ДЛЯ ПРОГНОЗУВАННЯ ДОРОЖНЬОГО ТРАФІКУ.....284

Насвіт Ю.О.
АНАЛІЗ ПІДХОДІВ ДО КЛАСТЕРИЗАЦІЇ В БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ 287

Якорнов Є.А., Цуканов О.Ф.
ВИЗНАЧЕННЯ КООРДИНАТ НАЗЕМНИХ РУХОМИХ ОБ'ЄКТІВ ЗА ДОПОМОГОЮ ГРУПИ БПЛА.....290

Лисенко О.І., Новіков В.І., Алєксєєва І.В.
МЕТОД ПІДВИЩЕННЯ ПРОПУСКНОЇ ЗДАТНОСТІ НЕОДНОРІДНОЇ МОБІЛЬНОЇ СЕНСОРНОЇ МЕРЕЖІ 293

Руренко О. Г., Корельчук Д.Г.
ПОРІВНЯННЯ ХМАРНИХ СЕРВІСІВ З КЛАСИЧНИМИ КЛІЄНТ-СЕРВЕРНИМИ АРХІТЕКТУРАМИ.....296

Вавринюк Д.С.
ВДОСКОНАЛЕННЯ АЛГОРИТМІВ СИНХРОНІЗАЦІЇ В МОБІЛЬНИХ СЕНСОРНИХ МЕРЕЖАХ 299

Filimonchuk V.M.
EXPLORATION OF EMISSION OF RADIO WAVES FOR MEANS OF COMMUNICATION AND CONTROL OF UNMANNED AERIAL VEHICLES.....302

Цуканов О.Ф., Якорнов Е.А.
ОЦІНКА ПАРАМЕТРІВ РУХУ ГРУПИ ПОСТІЙНО МАНЕВРУЮЧИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ 305

Тимофеєв Є.М., Лисенко О.І.
МЕТОДИ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ MIMO В МОБІЛЬНИХ СЕНСОРНИХ МЕРЕЖАХ 308

Руденко А.А., Курдеча В.В.
ПОРІВНЯННЯ ТЕХНОЛОГІЙ LI-FI ТА WI-FI У ВИКОРИСТАННІ ДЛЯ ТЕПЛИЧНОГО ГОСПОДАРСТВА 311

Терещенко О.В., Чмельов В. О.
ПІДСИСТЕМА ДЕКОРЕЛЯЦІЇ СИГНАЛІВ ВІД ПАСИВНИХ ЗАВАД В СУЧАСНИХ РАДІОЛОКАЦІЙНИХ СИСТЕМАХ 314

Явіся В.С., Лисенко О.І., Гетьман О.В.
КРИТЕРІЇ ВИБОРУ АЛГОРИТМІВ КЕРУВАННЯ ПОТОКАМИ ІНФОРМАЦІЙНИХ ПОВІДОМЛЕНЬ СЕНСОРНИХ МЕРЕЖ.....317

Фуртат С.О., Фуртат О.В., Гетьман О.В.
ПРОЦЕС ФУНКЦІОНУВАННЯ ПОВІТРЯНИХ РАДІОМЕРЕЖ ІЗ САМООРГАНІЗАЦІЄЮ FANET.....320

Валуйський С.В., Кравчук І.В.
МЕТОДИКА ПОБУДОВИ ЗАХИЩЕНОЇ МЕРЕЖІ НА ОСНОВІ ОБЛАДНАННЯ JUNIPER.....324

Валуйський С.В., Гірук Д.О.
АНАЛІЗ ФУНКЦІОНУВАННЯ ПРОТОКОЛУ OPENFLOW В ЛОКАЛЬНИХ МЕРЕЖАХ.....328

Валуйський С. В., Пономаренко І. О.
АЛГОРИТМ РОЗГОРТАННЯ ШЛЮЗІВ ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ РОЗУМНОГО ДОМУ 332

Соколов К.А., Жук С.Я.
АДАПТИВНА ТРАЄКТОРНА ФІЛЬТРАЦІЯ МАЛОРОЗМІРНОГО БПЛА ПРИ КОМПЛЕКСНОМУ ВИКОРИСТАННІ ДАНИХ РЛС І ВІДЕОКАМЕРИ 335

Олійник М.В.
ВИКОРИСТАННЯ ТЕХНОЛОГІЇ МІМО ДЛЯ ВИЯВЛЕННЯ ЦІЛЕЙ У СКЛАДНІЙ ЗАВАДОВІЙ ОБСТАНОВЦІ 338

Маленчик Т.В.
АНАЛІЗ ЕНЕРГЕТИЧНИХ ХАРАКТЕРИСТИК FMCW РАДАРУ МІЛІМЕТРОВОГО ДІАПАЗОНУ НА БАЗІ FPGA.....341

Вістизенко Є. В., Мовчанюк А.В.
АВТОНОМНИЙ ДАВАЧ СЕЙСМІЧНИХ ХВИЛЬ ДЛЯ ЗАДАЧІ ОХОРОНИ ПЕРИМЕТРА 344

Гримуд А.Г., Романюк В.А.
МОДЕЛЬ ПРИЙНЯТТЯ РІШЕННЯ ПО ТРАЄКТОРІЇ ПОЛЬОТУ ТЕЛЕКОМУНІКАЦІЙНОЮ АЕРОПЛАТФОРМОЮ ДЛЯ ЗБОРУ ДАНИХ МОНІТОРИНГУ З ВУЗЛІВ БЕЗПРОВОДОВОЇ СЕНСОРНОЇ МЕРЕЖІ 347

Blahaia O.S.
INVESTIGATION OF THE PHENOMENON OF RADIO RECEPTION BLOCKING OF UNPILOTED AERIAL VEHICLES.....350

П’ятнадцята 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;

ЛІСОВСЬКИЙ К.С.– представник студентської ради НН ІТС КПІ ім. Ігоря Сікорського.

Доповідачі:

Кравченко І.М. кер. Наритник Т.М.
ТЕНДЕНЦІЇ РОЗВИТКУ РАДІОРЕЛЕЙНИХ СИСТЕМ 355

Кисіль А. В. кер. Наритник Т.М
ІСТОРІЯ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ 4G-6 G ЗВ'ЯЗКУ У СВІТІ ..356

Луговець О.В. кер. Наритник Т.М.
СТАН ТА ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ТЕРАГЕРЦОВОГО ДІАПАЗОНУ В СУПУТНИКОВОМУ ЗВ’ЯЗКУ 357

Персіков М.А., Лемешко В.О., Мамон Р.В. кер. Єременко О.С.
ПРАКТИЧНЕ ВИКОРИСТАННЯ NETWORK DEVOPS ДЛЯ АВТОМАТИЗАЦІЇ УПРАВЛІННЯ В ІНФОКОМУНІКАЦІЯХ 358

Майба М.А. кер. Єременко О.С.
АНАЛІЗ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ СТЕГАНОГРАФІЧНОГО ПЕРЕТВОРЕННЯ 359

Негре Де Бофарулл Фернандо Рафаель, Юджесой Асіл Йігіт кер. Єременко О.С.
АНАЛІЗ І ДОСЛІДЖЕННЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ МЕРЕЖНОЇ БЕЗПЕКИ З УРАХУВАННЯМ БАЛАНСУВАННЯ НАВАНТАЖЕННЯ ..360

Юджесой Асіл Йігіт, Негре Де Бофарулл Фернандо Рафаель кер. Єременко О.С.
ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ТА БЕЗПЕКИ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ 361

Капуста Р.Д., Горяінова К.О. кер. Єременко О.С.
ПЕРЕВАГИ ВИКОРИСТАННЯ SIEM СИСТЕМИ WAZUH ДЛЯ ПІДВИЩЕННЯ СТІЙКОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА 362

Кашаіджа Джоель, Юджесой Асіл Йігіт, Негре Де Бофарулл Фернандо Рафаель кер. Єременко О.С.
ДОСЛІДЖЕННЯ АТАКИ "MAN-ON-THE-SIDE" ШЛЯХОМ МОДЕЛЮВАННЯ ЗАСОБАМИ WIRESHARK 363

Недоступ Д.М., Солом'яний М.В. кер. Єременко О.С.
СТРАТЕГІЇ ВІДМОВОСТІЙКОСТІ АРХІТЕКТУР EXTENDED CLOUD НА ОСНОВІ ПОЛІТИК 364

Тичинський - Мартинюк В.Ю. кер. Якорнов Є.А.
ВИМОГИ ДО ЕНЕРГЕТИЧНИХ ПАРАМЕТРІВ ІМІТАЦІЙНОЇ ЗАВАДИ КАНАЛУ УПРАВЛІННЯ ДРОНОМ.....365

Філімончук В.М. кер. Габрусенко Є.І.
ДОСЛІДЖЕННЯ ПОШИРЕННЯ РАДІОХВИЛЬ ДЛЯ ЗАСОБІВ ЗВ'ЯЗКУ ТА КЕРУВАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ...366

Благая О.С. кер. Габрусенко Є.І.
ДОСЛІДЖЕННЯ ЯВИЩА БЛОКУВАННЯ РАДІОПРИЙМАЛЬНОГО ПРИСТРОЮ БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТА 367

Орел М.В. кер. Курдеча В.В
ПРОБЛЕМИ УПРАВЛІННЯ БЕЗПРОВОДОВ 368

Кугут А.С. кер. Міночкін Д.А.
ПУБЛІЧНИЙ ХМАРНИЙ СЕРВІС.....369

Глоба А. А. кер. Носков В. І.
АНАЛІЗ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ QOS В МУЛЬТИСЕРВІСНИХ МЕРЕЖАХ ДОСТУПУ 370

Бушинський Д.А. кер. Курдеча В.В.
МОДИФІКОВАНА СИСТЕМА ЗАХИСТУ МЕРЕЖІ ІНТЕРНЕТ РЕЧЕЙ 371

Любарска С.І. кер. Курдеча В.В.
ПРОБЛЕМИ ОБРОБКИ ГРАФІЧНОЇ ІНФОРМАЦІЇ В МЕРЕЖІ IOT.....372

Корнійчук І.Г. кер. Курдеча В.В.
ЕНЕРГЕТИЧНЕ ПРОГНОЗУВАННЯ У ГІБРИДНИХ МІКРОМЕРЕЖАХ.....373

Кравченко Н. О. кер. Курдеча В.В.
ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ТРАНСПОРТНОЇ ЛОГІСТИКИ НА ОСНОВІ ІНТЕРНЕТУ РЕЧЕЙ 374

Сахнюк О.Р. кер. Курдеча В.В.
ПРОБЛЕМИ ВІРТУАЛІЗАЦІЇ В МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ.....375

Петровський Д. С. кер. Курдеча В.В.
ПОРІВНЯННЯ МЕТОДІВ ЗБОРУ ТА ОБРОБКИ ІНФОРМАЦІЇ В СЕНСОРНІЙ МЕРЕЖІ 376

Ткаченко В.М. кер. Курдеча В.В
АНАЛІЗ ПРОБЛЕМИ МАСШТАБОВАНОСТІ МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ 377

Лагода А.В. кер. Носков В. І.
МЕРЕЖА ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ КЕРУВАННЯ ДОРОЖНІМ РУХОМ 378

Мельник В.В. кер. Курдеча В.В.
МЕТОД КОНТРОЛЮ ЯКОСТІ ЗВ'ЯЗКУ В МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ НА ОСНОВІ БЕЗПРОВОДОВИХ ТЕХНОЛОГІЙ 379

Ковальська Д.Д. кер. Курдеча В.В.
МЕТОД АУДИТУ ІНФОКОМУНІКАЦІЙНОЇ МЕРЕЖІ ВЕЛИКИХ ПІДПРИЄМСТВ 380

Семінар "Інноваційна діяльність студентів НН ІТС"

Співголови: Новогрудська Р.Л. – к.т.н., доц., Лісовський К.С.

Доповідачі:

Кириндась Н.П. кер. Валуйський С.В.
ПЕРСПЕКТИВИ РОЗВИТКУ ТЕХНОЛОГІЇ FIREWALL У КОНТЕКСТІ РОЗВИТКУ ГЛОБАЛЬНОЇ МЕРЕЖІ ТА ЗРОСТАННЯ ОБ'ЄМУ ІНФОРМАЦІЇ 381

Лісовський К.С. кер. Живков О.П.
ТЕСТУВАННЯ ТА ІМПЛЕМЕНТАЦІЯ ТЕХНОЛОГІЇ СУПУТНИКОВОГО ЗВ'ЯЗКУ STARLINK У СУЧАСНИХ УМОВАХ ВИКОРИСТАННЯ.....382

Шелест Є.В. кер. Живков О.П.
РОЗРАХУНОК ТА ПРАКТИЧНА ПЕРЕВІРКА ЗАВАД ПЕРЕДАЧІ ДАНИХ У СИСТЕМІ СУПУТНИКОВОГО ЗВ'ЯЗКУ STARLINK В УМОВАХ СУЧАСНОГО ВИКОРИСТАННЯ.....383

Kostiantyn Lisovskyi, Gleb-David Rochenovich кер. Dr. Muhammad Rizky Prima Sakti
POTENTIAL DEVELOPMENT & IMPLEMENTING OF BLOCKCHAIN AND CRYPTOCURRENCIES IN THE EUROPEAN UNION AND THE EUROZONE (INCLUDING UKRAINE) 384

Mykhaylo Gavryliv кер. Prof. John Wetherell
APPLYING THE MARSHALL PLAN TO UKRAINE'S ECONOMIC RECOVERY AFTER THE WAR.....385

Пленарні доповіді

До 100-річчя академіка Глушкова В.М.

ПРОДОВЖЕННЯ СПРАВИ АКАДЕМІКА ГЛУШКОВА В.М. У РОЗВИТКУ СУЧАСНИХ ІНФО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Ільченко М.Ю., Кравчук С.О., Уривський Л.О.

Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Навчально-науковий інститут телекомунікаційних систем, м. Київ, Україна
E-mail: leonid_uic@ukr.net

CONTINUATION OF THE CASE OF ACADEMICIAN GLUSHKOV V.M. IN THE DEVELOPMENT OF MODERN INFORMATION & COMMUNICATION TECHNOLOGIES

The outstanding contribution of Academician Glushkov V.M. into the theory and practice of creating automated control systems on a national scale makes the achievements of a scientist and organizer of science relevant and important. Significant achievements, promising developments, recognized scientific schools of Igor Sikorsky Kyiv Polytechnic Institute in the most important areas of fundamental and applied scientific research in the field of information technology were noted. The leader of the implementation of current and promising developments and achievements in the information and telecommunication sphere in our university is ES ITS.

Неможливо переоцінити ту спадщину, яку залишив у вітчизняній та світовій науці та техніці академік В.М. Глушков [1], 100-річчя із дня народження якого зустрічає у цьому році всесвітня наукова спільнота. За справедливим висловом академіка І.В. Сергієнка [2-3], ми ясно бачимо, що В.М. Глушков набагато раніше від більшості своїх колег зумів оцінити важливість та перспективність використання комп'ютеризованих систем управління та моделювання у різноманітних сферах економіки країни. Саме видатний внесок у теорію та практику створення автоматизованих систем управління державного масштабу робить актуальними та важливими досягнення вченого та організатора науки.

Під його керівництвом у 1966 р. була розроблена перша персональна електронно-обчислювальна машина (ЕОМ) «МИР-1» як спеціалізована обчислювальна машина (прообраз комп’ютера) для інженерних розрахунків [1,3].

У 1973 р. В.М. Глушков підтримав і розвинув революційну ідею створення мережі ЕОМ з пакетною комутацією каналів на основі радіоканалів, що дозволило об'єднувати на рівноправній основі великі ЕОМ та віддалені термінали на площі десятки квадратних кілометрів [4].

У сучасному світі простір телекомунікацій переживає епоху бурхливої еволюції, потенціал якої накопичувався протягом останніх трьох десятиліть. Така еволюція проявляється у кількох важливих напрямах.

Головним із цих напрямів слід вважати тенденцію до злиття раніше незалежних один від одного технологій: інформаційних та комунікаційних.

Академіку В.М. Глушкову належить воістину пророче висловлювання (1982 р.): «Безпаперова інформатика розвивається виключно швидкими темпами <…>. Зрощування засобів телекомунікацій з машинною інформатикою (що реалізується в мережах ЕОМ та ВЦ з віддаленими терміналами) вже призвело до появи нового терміну *телематика*. Найбільш завзяті апологети телематики пророкують, що вже недалекий той день, коли зникнуть звичайні книги, газети та журнали. Натомість кожна людина буде носити з собою «електронний» блокнот, що є комбінацією плоского дисплея з мініатюрним радіопередавачем. Набираючи на клавіатурі цього блокноту потрібний код, можна (перебуваючи в будь-якому місці на нашій планеті), викликати з гігантських комп'ютерних баз даних, пов'язаних у мережі, будь-які тексти, зображення (у тому числі і динамічні), які і замінять не тільки сучасні книги, журнали та газети, але й сучасні телевізори. Прогрес електронної технології, машинної інформатики та телематики відбувається настільки бурхливими темпами, що фантастика у цій галузі стає реальністю буквально на наших очах» [5].

У сучасній практиці термін «телематика» (телекомунікації + інформатика) найчастіше вживається у конструкції «інфокомунікації» (інформатика + телекомунікації).

Прямим продовженням справи, розпочатої академіком В.М. Глушковим. є сучасні інфокомунікаційні стратегії і технології, пов'язані з реалізацією в Україні глобальної концепції розвитку інформаційного суспільства [6-8].

Відповідно до Окінавської Хартії глобального інформаційного суспільства [9], інформаційно-комунікаційні технології (ІКТ) є одним із найважливіших факторів, що впливають на формування суспільства двадцять першого століття. Їх революційний вплив стосується способу життя людей, їхньої освіти та роботи, а також взаємодії уряду та громадянського суспільства.

Кожна людина повинна мати можливість доступу до інформаційних та комунікаційних мереж.

Ключовою складовою цієї стратегії має стати безперервний рух у напрямку загального доступу для всіх. Тому найбільш динамічно розвинутою гілкою сучасних комунікацій став Інтернет як вершина «безпаперової інформатики».

Інтернет в наш час перетворився на один із ключових елементів людського життя. Сьогодні він є широко доступним на смартфонах та інших мобільних пристроях.

У 2022 році [10] інтернет використовувався переважно для спілкування з іншими людьми, надсилання/отримання електронних листів (77%), обміну миттєвими повідомленнями (72%), пошуку інформації про товари та послуги (70%), здійснення голосових чи відеодзвінків (66%) і перегляду потокового телебачення чи відео онлайн (65%).

На рівні ЄС у 2022 році 24% отримували доступ до особистих медичних записів онлайн та ще 18% використовували інтернет, аби отримати доступ до

інших медичних послуг через web-сайт або застосунок замість того, щоб йти до лікарні чи відвідувати приватного лікаря.

Україна, наслідуючи глобальні тенденції, розвиває інфокомунікаційні технології з урахуванням новітніх світових досягнень.

Структура доходів від надання послуг телекомунікацій в Україні відповідає світовим тенденціям (рис. 1) [11].

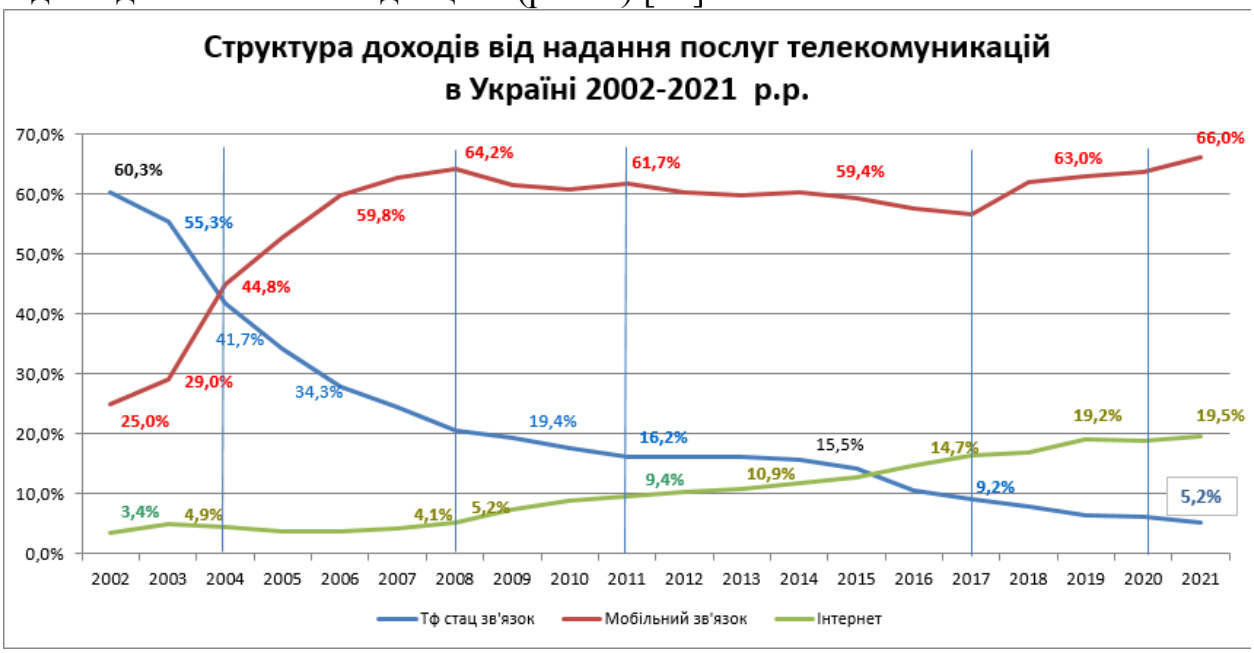


Рис.1. Структура доходів від надання послуг телекомунікацій в Україні 2002-2021 р.р.

За кількістю користувачів Інтернету Україна посідає гідне місце у світі [12] (Таблиця 1), зокрема, за відсотком користувачів від загальної чисельності населення.

Таблиця 1. Світова статистика користувачів Інтернету станом на травень 2022 року.

Країна	Кори стувачів Інтернету, млн.	Відсоток населення
Китай	1010,7	69,8
Індія	833,7	59,5
США	312,3	93,4
Японія	118,6	93,3
Німеччина	79,1	94,0
Україна	40,9	94,5

Будучи математиком за освітою, В.М. Глушков виявив разючу прозорливість у складних питаннях управління економікою. Тому не менш важливою стратегічною тенденцією є передбачений В.М. Глушковим взаємозв'язок інформатики та економіки, що проявляється в умовах динаміки інформаційного суспільства в синхронному розвитку економіки та електронних комунікацій.

Розвиток концепції побудови «інформаційного суспільства», у якій головними продуктами виробництва стають інформація та знання, неможливе без наукових новацій у галузі теорії інформації.

Реальним відображенням втілення згаданої концепції є процеси, об'єднані поняттям «інформатизація» та спрямовані на побудову та розвиток комунікаційної інфраструктури, що поєднує територіально розподілені інформаційні ресурси.

У світовому інформаційному просторі стало розвіваються цілий спектр новітніх технологій і пов'язаних із цим застосувань [7]:

– впровадження 5G;
– розвиток Інтернету речей (IoT);
– інформаційно-комунікаційні технології в процесах «Індустріалізації 4.0»;
– розвиток нейронних мереж та штучного інтелекту.

З 22 травня 2019 р. в Україні запрацювала система електронної взаємодії «Трембіта». 125 державних послуг доступні на урядовому порталі та повністю автоматизовані. Державні закупівлі, приватизація, звіти про технічну допомогу та держпідприємства – усі ці послуги доступні онлайн для кожного українця.

«Наша мета – країна в смартфоні», – сказав президент В. Зеленський [13].

У 2020 році офіційно запущено мобільний застосунок, вебпортал і бренд цифрової держави в Україні, розроблений Міністерством цифрової трансформації України – «Дія» (скорочення від «Держава і я») .

До 2024 року 75% населення повинні мати можливість користуватися надійними та безпечними засобами eID, адже понад 90% державних служб країни працюватиме онлайн [14].

Одним із активних учасників процесу розвитку сучасних телекомунікаційних стратегій є Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», який має значні здобутки, перспективні розробки, визнані наукові школи з найважливіших напрямів фундаментальних та прикладних наукових досліджень у галузі інформаційних технологій:

– сучасні методи обробки інформації, принципи побудови високопродуктивних обчислювальних систем та мереж, перспективні інформаційні технології обробки інформації, діагностики та управління у складних організаційно-технічних системах;

– апаратне, математичне та програмне забезпечення цифрових систем у сучасних інформаційних технологіях, методологія та методи побудови інтелектуалізованих інформаційних – та мережних технологій, баз даних та знань;

– перспективні системи електронних комунікацій і технології на основі сучасної мікрохвильової та цифрової електронної техніки;

– методи структурно-параметричної оптимізації електродинамічних систем та створення нових радіотехнічних, електроакустичних, мікроелектронних пристроїв.

Одним із визнаних лідерів імплементації сучасних і перспективних розробок та досліджень у інформаційно-комунікаційної сфері є НН ІТС КПІ ім. Ігоря Сікорського, в якому склалися багаторічні традиції розвитку наукової школи, яку створив і очолив засновник і науковий керівник НН ІТС, академік НАН України д.т.н., професор Ільченко М.Ю. Вихованцями школи стали 8 докторів технічних наук, 37 кандидатів технічних наук.

Вклад вчених НН ІТС у розвитку ті поширенню ідей побудови сучасного інформаційного простору в Україні був високо оціненим Президією НАН України. В присутності академіка Патона Б.Є. дипломи Премії імені Глушкова В.М. в 2019 р. отримали професори Ільченко М.Ю., Кравчук С.О., Уривський Л.О.

Новим етапом зростання вагомості наукового вкладу молодого покоління дослідників в сфері інформаційно-телекомунікаційних технологій став перехід до підготовки докторів філософії за спеціальністю 172 Телекомунікації та радіотехніка. Перші захисти дисертацій випускників нового покоління аспірантури мають пройти в квітні 2023 р.

В НН ІТС і НДІ телекомунікацій, який з 2001 року працює під науково-технічним керівництвом Відділення інформатики НАН України, активно працюють 8 наукових груп, які очолюють провідні вчені. Керівниками студентських науково-технічних гуртків виступають, як правило, молоді вчені.

За офіційним даним МОН У, НН ІТС займає лідерську позицію в Україні стосовно обсягів виконання державного замовлення щодо підготовки фахівців вищого рівня за спеціальністю «Електронні комунікації та радіотехніка». Державне замовлення МОН Украйни за цією спеціальністю виконує майже 40 університетів країни. Серед них частка НН ІТС в прийомі до бакалаврату в 2020, 2021, 2022 роках склала 180 осіб або 13% від обсягу державного замовлення.

У цьому проявляється наступність поколінь, запорука реалізації чудових ідей, заповіданих нам академіком В.М. Глушковим.

Висновки

1. Ядро наукової спадщини академіка В.М. Глушкова складають важливі народногосподарські об'єкти:

– вперше створені високопродуктивні обчислювальні засоби;

– реалізовані в державному масштабі автоматизовані системи управління економікою;

– відтворені мережі передачі інформації по радіоканалам як прообрази сучасних безпроводових телекомунікацій;

– теоретичні засади організації безпаперової інформатики.

2. Прямим продовженням справи, розпочатої академіком В.М. Глушковим, є реалізація сучасних інфокомунікаційних технологічних напрямів, пов'язаних з їх втіленням в Україні:

– Глобальної концепції розвитку інформаційного суспільства;

– тісного взаємозв'язку інформатики та економіки, що передбачає, зокрема, синхронний розвиток економіки та телекомунікацій;

– всеукраїнської технологічної стратегії «Держава у смартфоні»;

– розвитку кібернетики як науки, включаючи аспекти прикладної теорії інформації.

3. НН ІТС та НДІ телекомунікацій разом з іншими науковими та навчальними організаціями беруть активну участь у розвитку сучасних телекомунікаційних стратегій:

– через участь у виконанні науково-технічних проектів і завдань у сфері інформатизації;

– теоретичний та практичний розвиток засобів передачі інформації за допомогою електронних комунікацій;

– реалізація концепції NGN та FGN у навчальному процесі при формуванні професійного вигляду сучасного випускника вишу у сфері інформатизації.

Література

1. Вікіпедія: Глушков Віктор Михайлович // https://uk.wikipedia.org/wiki/Глушков_Віктор_Михайлович.
2. Сергієнко І.В. Академік Глушков і справа його життя // Дзеркало тижня. – 2003. – № 31, 16 серпня.
3. Сергієнко І.В. Наукові ідеї академіка В.М. Глушкова та розвиток сучасної інформатики // Вісн. НАН України. – 2008. – № 11. – С. 35–60, № 12. – С. 9–29.
4. Ільченко М.Ю. Проблеми телекомунікаційного забезпечення інформатизації держави // Праці Міжнар. конф. «50 років Інституту кібернетики імені В.М. Глушкова НАН України». – К.: ІК ім. В.М. Глушкова НАН України, 2008. – С. 75–84.
5. Ilchenko M., Uryvsky L. Development of the scientific heritage of academician V.M. Glushkov in modern telecommunication strategies / Cybernetics and Systems Analysis. International Theoretical Science Journal. – 2013, Vol.49, № 4. – p.p. 76…87.
6. Ільченко М.Ю., Кравчук С.О. Сучасні телекомунікаційні системи. – К.: Наук. думка, 2008. 328 с.
7. Ilchenko M., Uryvsky L., Osypchuk S. The Main Directions of Improving Infocommunications in the Global Tendencies // Advances in Information and Communication Technologies. Lecture Notes in Networks and Systems / monograph. – Springer, Cham, 2020. – p.p. 3-22. https://link.springer.com/book/10.1007/978-3-030-58359-0.
8. Ilchenko M., Uryvsky L. Aspects of systems analysis in the applied information theory for telecommunications / Cybernetics and Systems Analysis. International Theoretical Science Journal. – 2010, Vol.46, № 5. – p.p. 60-67.
9. Okinawa Charter on Global Information Society. – Ministry of Foreign Affairs of Japan //https://www.mofa.go.jp/policy/economy/summit/2000/documents/charter.html
10. https://mediasat.info/
11. Офіційний сайт Держкомстату України www.ukrstat.gov.ua/
12. Europe Internet Users and Population Statistics // https://www.internetworldstats.com/stats4.htm
13. https://www.president.gov.ua/news/volodimir-zelenskij-dodatok-diya-ce-pershij-krok-na-shlyahu-59633
14. https://tech.liga.net/technology/novosti/u-zelenskogorasskazali-kak-budut-perevodit-gosuslugi-v-onlayn

1000+ НОВИНИ ІНФОТЕЛЕКОМУ

Кононова І.В.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: viti21@ukr.net

1000+ INFOTELECOM NEWS

The main news for 2022-2023 in the field of information and communication technologies are summarized. The main trends and development of key modern technologies are presented in Ukraine and the world. This material was prepared for students, teachers and engineers.

Нині важко навіть уявити, як люди могли колись обходитися без телефону та Інтернету, адже ці речі стали для нас невід'ємною часткою життя, вони надають безмежні можливості для спілкування, обміну інформацією, пізнання нового та збереження інтелектуальних і наукових надбань. А доступність до телекомунікаційних мереж та інформаційних ресурсів давно вже стала мірилом зрілості суспільства, його здатності реагувати на виклики часу. Динамічний розвиток телекомунікаційної галузі потребує постійного корегування регулятивного середовища, формування новітніх підходів до створення найкращих умов розвитку технологічних інновацій.

Оскільки Навчально-наукового інституту телекомунікаційних систем КПІ ім. Ігоря Сікорського готує фахівців за спеціальністю 172 Телекомунікації та радіотехніка ми систематично подаємо в нашому телеграм каналі Деканат ІТС та на сайті НН ІТС інформацію про новини в сфері телекомунікацій.

За весь період створення новин інфотелекому було опубліковано: 1326 новин.

В 2020 році – 333 новини, в 2021 році – 486 новин, 2022 році – 459 новин.

З початку 2023 року – 48 новин.

Сучасні тенденції розвитку у світовій сфері телекомунікації можна охарактеризувати як перехід до глобалізації, створення єдиного інформаційного простору, єдиної уніфікованої системи телекомунікацій та стандартів, обміну інформацією, впровадження нових інформаційних технологій у всі сфери життя суспільства. А бурхливий розвиток

телекомунікацій – це необхідна умова створення бізнес-інфраструктури та розвиток сучасних інформаційних технологій.

Як одним з найбільших прикладів бурхливого розвитку телекомунікацій став Рік незламності Мінцифри, який показав усьому світу, що цифрова трансформація працює і під час війни.

В цьому році розділемо новини інфотолекому на наступні розділи: штучний інтелект (ШІ), Інтернет речей (IoT), хмарні обчислення, блокчейн, великі дані (Big Data) адже це вже наша нова реальність.

Поява науки про великі дані як галузі вивчення та практичного застосування за останнє століття призвела до розвитку таких технологій, як глибоке навчання, обробка природної мови та комп'ютерний зір. Це дозволило з'явитися машинному навчанню як способу роботи над тим, що ми називаємо штучним інтелектом, областю технологій, яка швидко змінює те, як ми працюємо та живемо.

Штучний інтелект є однією з ключових технологій сучасності. Понад 50 країн світу, а також Північноатлантичний альянс, вже створили й затвердили власні стратегії розвитку штучного інтелекту, щоб зафіксувати свої завдання й пріоритети у цій сфері, прискорити темпи свого науково-технічного та соціально-економічного розвитку.

У світі відбувається нова технологічна революція, яка розгортається на основі інтеграції зазначених технологій практично в усі сфери економіки й соціального життя. Формується фактично новий тип суспільства (Суспільство 5.0), виробничі ланцюжки якого, логістика, соціальна інфраструктура будуть базуватися на ШІ. У найближчому майбутньому озброєність інтелектуальними технологіями, інтенсивність і ефективність їх упровадження стануть критерієм розвиненості тієї чи іншої національної економіки. Відповідно привабливість країн і регіонів, концентрація в них кваліфікованої робочої сили, об'єктів високотехнологічного виробництва, матеріальних і фінансових ресурсів, освітніх установ, інфраструктурних і культурних об'єктів залежатиме від ступеня впровадження ШІ. Різні країни бачать подібні можливості у сфері розвитку та впровадження штучного інтелекту. У їхніх планах, концепціях і стратегіях найчастіше підкреслюється, що охорона здоров'я, технології, сільське господарство й виробництво є секторами з найбільшим потенціалом трансформацій за допомогою ШІ.

Уряди всіх країн розуміють потенціал цієї технології для збереження й можливого просування своїх конкурентних позицій в основних галузях промисловості, а стратегія розвитку штучного інтелекту в Україні передбачає можливість використання різних моделей і підходів, які сприятимуть

створенню проривних технологій у сфері ШІ, зокрема квантових і нейроподібних комп'ютерів, систем машинного навчання.

Отже, вирішення проблем розвитку та ефективного використання систем знань у різних галузях людської діяльності, як свідчить світовий досвід, лежить у площині застосування сучасних інформаційних технологій, що реалізуються на засадах штучного інтелекту як однієї з ключових технологій сучасності.

Інтернет речей. Бурхливий розвиток технічних засобів і підвищення активності доступу до інформаційно-обчислювальних ресурсів підвищили інтерес до проблеми ефективного використання мережевих ресурсів IoT і забезпечення оперативного доступу до них.

На даний час пристрої IoT не лише масово використовуються у щоденному вжитку, але й у сучасному бізнес-середовищі. Зокрема Інтернет речей активно впроваджується в різних галузях — від промислової сфери до сільського господарства, рітейлу та будівництва. А зростання кількості пристроїв IoT спричиняє виникнення нових проблем проєктування, застосування, експлуатації та безпеки. Бурхливий розвиток технічних засобів і підвищення активності доступу до інформаційно-обчислювальних ресурсів підвищили інтерес до проблеми ефективного використання мережевих ресурсів Інтернету речей і забезпечення оперативного доступу до них.

Популярними сьогодні стають так звані «розумні речі», або Smart речі. Наприклад, гаджети, які зручно носити з собою, мають невеликі розміри і незначну масу — «розумний» годинник, фітнес-трекери, смарт-окуляри, гнучкі екрани, а «розумні будинки» дають змогу ефективно керувати всіма системами функціонування будівлі за допомогою дистанційних пультів і мобільних телефонів, оптимально витрачати тепло, воду, світло тощо. Усе це створює у світі умови для нового явища — Інтернету майбутнього, що включає в себе, крім нинішнього Інтернету людей (Internet of People, IoP), ще й Інтернет речей (Internet of Things, IoT), Інтернет медіаконтенту (Internet of Media, IoM), Інтернет сервісів (Internet of Services, IoS).

Метою даного блоку новин є інформування викладачів та інженерно-технічних працівників, що займаються науковими розробками і проєктуванням в області Інтернету речей та інформаційних систем й технологій, а також для аспірантів і студентів, які цікавляться даними питаннями.

Хмарні обчислення один з провідних трендів в світі IT-протягом останніх років. Вони являють собою реальне зрушення парадигми в розгортанні обчислювальних систем. Хмарні обчислення роблять реальністю давню мрію про нескінченно масштабовану, загальнодоступну систему

обчислень, що докорінно змінило наш спосіб життя. А парадигма хмарних обчислень передбачає, що ресурси – віртуальні і безмежні, що деталі фізичних систем, на яких працює програмне забезпечення абстрагуються від користувача.

В даному розділі новин інфотелекому ви зможете дізнатись відповіді на головні питання:

Скільки даних наразі зберігається в хмарі?

Хто є найбільшим провайдером хмарних сервісів?

Для чого найчастіше використовуються хмарні технології?

Який дата-центр є найбільшим у світі?

Хмари — публічні, приватні чи гібридні?

Який відсоток компаній зберігає конфіденційні дані у хмарі?

Яким чином зростання темпів запровадження хмарних рішень вплине на ринок IT-інфраструктури?

Як змінився попит на професії, пов'язані з хмарними обчисленнями?

Який вплив на хмару має штучний інтелект?

Блокчейн – одна з трендових технологій сьогодення, яка дає змогу відкрити дані й продемонструвати, що вони не зазнали змін, не розкриваючи при цьому персональні дані користувачів.

Інтерес до технології блокчейн виявляють IT-компанії та вивчають можливості її застосування всюди — від фінансів до виробництва:

Корпорація Microsoft розвиває програми Blockchain-as-a-Service (BaaS) на своїй хмарній платформі Azure;

IBM запустила власну BaaS пропозицію; передбачається його інтеграція з іншими продуктами компанії, такими як обчислювальна мережа IBM z Systems, система штучного інтелекту Watson для Інтернету речей та ін.;

Blockchain Foundry приділяє головну увагу заснованим на блокчейн сервісам для створення прототипів і випуску промислової продукції;

Bigchain DB пропонує масштабовані сервіси блокчейн;

Chain рекламує платформу блокчейн для фінансових сервісів;

IBM і Samsung працюють над концепцією ADEPT, в якій технологія блокчейн буде використовуватися для формування основи децентралізованої мережі пристроїв — Інтернету речей. Блокчейн планують використовувати для реєстрації мільярдів пристроїв, які будуть автономно транслювати транзакції в системі з трирівневою архітектурою.

Революція в сфері даних обумовлена активним накопиченням обсягів даних, необхідністю їх зберігання та обробки. Існуючі технології відставали від потреб користувачів, що привело до створення концепції «великих даних». **Big Data** – це горизонтально масштабована система, яка

використовує набір методик і технологій, що дозволяють обробляти структуровану і неструктуровану інформацію зі значного масиву даних, формувати відповідні зв'язки для інтерпретації. Для «великих даних» характерними є п'ять ознак:

volume – обсяг даних вважається великим, коли виникають труднощі при обробці цього обсягу засобами традиційних систем управління базами даних (більше 1 петабайт);

velocity – швидкість обробки даних, в тому числі, і в режимі реального часу;

variety – інформація великих обсягів дуже рідко буває однорідною. У переважній більшості випадків загальний масив даних включає як структуровані, так і неструктуровані дані;

veracity – здатність виділити і відсіяти корисну складову даних від інформаційного «шуму»;

value – цінність інформації визначає доцільність її обробки. Зібрані дані повинні давати відповіді на заздалегідь сформульовані питання і ті, що з'являються знову.

Вони використовуються в технологіях когнітивних розрахунків, здатних оброблювати неструктуровану інформацію без заздалегідь наданого алгоритму.

Потенціал, який відкривають технології Big Data, а потім і розумних даних, виходить за рамки сучасного розуміння про інформацію. У той час, коли великі технологічні компанії таких як Google, Microsoft, Amazon, Facebook та ще цілий ряд великих компаній вже активно використовують їх.

Слідкуйте за нашими новинами та будьте в курсі головних подій та трендів IT-ринку.

UDC 621.38

SCINTILLATION DETECTORS BASED ON NaI:Tl WITH 3% RESOLUTION IN CLASSIFICATION TASKS USING NEURAL NETWORKS

Suzdal V.I., Tavrovskyi I.S.
KTH Roial Instinute Of Tehnology, Stockholm
E-mail: suzdal170478@gmail.com

СЦИНТИЛЯЦІЙНІ СЕНСОРИ НА КРИСТАЛІ NAI:TL З 3% РОЗДІЛЬНОЮ ЗДАТНІСТЮ В ЗАДАЧАХ КЛАСИФІКАЦІЇ НЕЙРОННИМИ МЕРЕЖАМИ

У роботі розглянуто використання нейронних мереж для обробки гамма-спектрів, що призводить до покращення процесу ідентифікації ізотопів та зменшення часу, необхідного для аналізу. Це забезпечує більш високу точність ідентифікації ізотопів, швидшу та більш автоматизовану, оскільки не вимагає повторного процесу розкладання та реконструкції спектра.

In the paper using of neural networks for processing gamma spectra leads to an improvement in the process of isotope identification and a reduction in the time required for analysis are considered. It allows for a higher accuracy in isotope identification, faster and more automated, as it does not require the repetitive process of spectrum decomposition and reconstruction.

Keywords: energy resolution, neural networks, nucleus.

Modern gamma spectroscopy provides unique opportunities for conducting various studies in many areas of knowledge. The main task of spectroscopic measurements is to determine the energy, intensity of discrete gamma lines from various gamma sources, their identification, and localization. Such studies are often carried out using scintillation detectors based on inorganic crystals such as NaI:Tl, CsI:Tl, and others. These detectors are widely used due to their high sensitivity and good operational properties. However, the insufficiently high energy resolution of scintillation detectors (SD) based on inorganic crystals (at best 6-7% for gamma quanta with an energy of 662 keV) does not allow solving many of the above-mentioned tasks to the fullest extent.

There are many ways and already implemented software products with classical approaches for processing radiation spectra. However, a relevant and actively developing issue today is the question of applying the paradigm of artificial neural networks for this purpose [1].

A successful solution to the problem of isotope identification using neural networks has been presented in the work of Ukrainian scientists A.V. Kochergin and S.S. Pivovarcev [2]. Based on the recommendations of these authors, a method of identifying radionuclides using a three-layer feedforward neural network was

used. The authors [2] draw attention to the fact that the temporal constraints of the measurement and identification procedure lead to the fact that in most cases the resulting gamma spectrum has a complex character with a significant number of multiples. These multiples are difficult to identify at real count rate levels that are only slightly higher than the detector's background load. The number of simultaneously identified isotopes cannot be large, so it is recommended to limit the number of simultaneously identifiable nuclides. To overcome the alone-stated problem, it was decided to use a multi-pass identification procedure with a NaI:Tl crystal detector, and a neural network architecture using the Sequential class from Keras. To construct the neural network, one hidden layer of neurons was defined and the activation function of the output layer with one neuron and a sigmoid activation function was determined. The model was compiled using a binary cross-entropy loss function, the Adam optimizer, and accuracy as the metric. The model was trined using the fitting method. We calculated the predictions. The output was an array of predicted probabilities for each input vector with values ranging from 0 to 1. The developments were carried out in Python, using libraries for scientific data processing, such as Keras, Theano, Tensorflow, and others.

An artificial neural network trained on the simple linear spectra showed results close to 95% for identifying individual nuclides. However, identifying nuclides with complex linear spectra yielded ambiguous results. To further develop the identification method, it was decided to use a NaI:Tl crystal detector spectrum with 3% resolution and isolate the energy range of interest to build and train a separate artificial neural network for it.

Figure 1 shows the radiation spectrum obtained by the crystal detector of dimensions 25x25 mm. The energy resolution at the peak of full absorption is 8.6%. The processed spectrum is shown in Figure 2, with an energy resolution at the peak of full absorption as 3.3%.

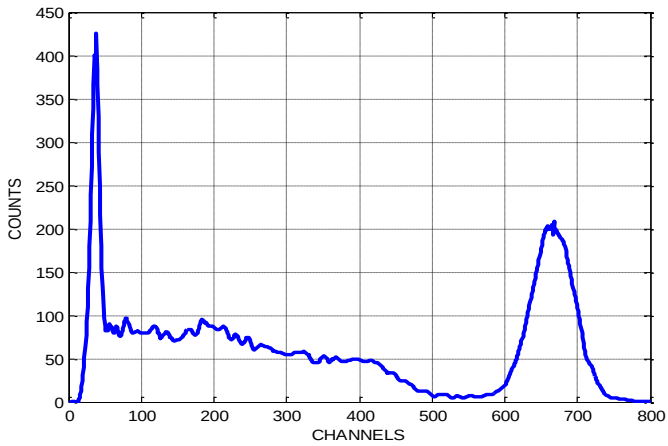


Fig.1. Radiation spectrum Cs^{137}.

To obtain the NaI:Tl crystal detector spectrum with 3% resolution, an algorithm for obtaining and analyzing the fine structure of the detector's output

pulses was proposed [3.4]. A mathematical model was assigned to each scintillation pulse. The idea of further research was to decompose (cluster) the set of pulses into groups based on the shape of each pulse. Similar events, such as those with similar attenuation, combustion characteristics, maximum amplitude, etc., were selected for each group. The mathematical measure of similarity was a norm, the choice of which allows controlling the criterion for group formation.

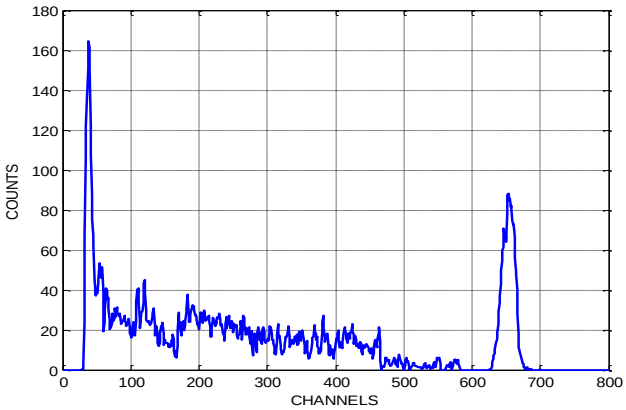


Fig.2. Gamma spectrum obtained on the crystal after processing.
The energy resolution at the peak of total absorption is 3.3%.

Using a neural network to identify the isotope Ba133 based on the NaI:Tl crystal detector spectrum with 3% resolution yielded results close to 100%. Identifying nuclides with complex linear spectra showed results close to 40%.
The multi-pass identification procedure method is a good approach for addressing problems associated with a large number of multiplexes in the gamma spectrum. The binary cross-entropy loss function and Adam optimizer are common choices for training neural networks, as they show good results in most machine learning tasks.

References

1. Levy R, Cohn, S. B. A History of Microwave Filter Research. IEEE Transactions on Microwave Theory and Techniques, 1984, p 1055–1067
2. A.V. Zakharov, M.E. Ilchenko, Mixed bonds in microstrip band pass filters. Radio engineering and electronics № 6, 2018, p. 607–618,
3. J.S. Hong, M.J. Lancaster, Microstrip cross-coupled trisection bandpass filters with asymmetric frequency characteristics, IEE Proc.- Microw. Antennas Propag, vol. 146, no. 1, p. 84–90, 1999
4. R. Levy, New cascaded trisections with resonant cross, MTT-S Int. Microwave, vol. 2, p. 447–450, 2004
5. M.E. Ilchenko, A. P. Zhivkov. Bridge Equivalent Circuits for Microwave Filters and Fano Resonance, Advances in Communication Technologies. Springer, 2019, p. 278-298
6. Warren P. Mason Electromechanical Transducers. Van Nostrand Company, Inc., 1942
7. Guillemin, E.A. Synthesis of Passive Networks: Theory and Methods Appropriate to the Realization and Approximation Problems. Wiley, Hoboken, 1957
8. http://f1chf.free.fr/hyper/Design%20de%20filtre.pdf
9. David M. Pozar. Microwave Engineering. Wiley, 2011, P. 752.

УДК 621.382

АНАЛІЗ ПОТЕНЦІЙНИХ ВРАЗЛИВОСТЕЙ ТА ЗАГРОЗ В 5G

Правило В.В.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: v.v.pravylo@ukr.net

ANALYSIS OF POTENTIAL VULNERABILITIES AND THREATS IN 5G

Vulnerabilities of 5G networks and critical infrastructure are considered. The criticality classification of 5G infrastructure assets is given.

З поточних опублікованих стандартів і досліджень, проведених в співтоваристві 5G, були виявлені деякі помітні вразливості. Ці уразливості можуть бути усунені в майбутніх випусках стандартів, і очікується, що деякі з них будуть усунені після завершення розробки стандартів 5G. Вразливості розбиті на три розділи: конфіденційність, цілісність і доступність (CIA). Тріада CIA, як відомо, є наріжним каменем політики безпеки і визначає найбільш важливі компоненти безпеки. Цілком імовірно, що деякі з них будуть розглянуті в майбутньому, однак деякі висновки буде важко пом'якшити, і станом на випуск 15 3GPP вони як і раніше вразливі [1].

Конфіденційність. Конфіденційність − це принцип, згідно з яким конфіденційні дані не будуть передані сторонам, які не мають потреби або повноважень на доступ. У разі стільникового зв’язку це може означати текстові повідомлення, телефонні дзвінки та інтернет-трафік. У просторі 5G з IoT це може означати медичні пристрої, які збирають дані для практикуючих лікарів, або обладнання для управління будівлею, яке дозволяє входити в територію. Важливо, щоб ці дані були захищені від загроз, щоб запобігти ненавмисному витоку персональних даних або даних безпеки [2].

Цілісність. Цілісність − це принцип підтримки точності та узгодженості даних від кінцевої точки до точки, і це важливо для бездротового зв’язку, щоб запобігти маніпуляціям даними через фактори навколишнього середовища або зловмисних суб’єктів. Специфікації бездротового зв’язку часто включають методи повторної передачі даних, щоб подолати розриви або перешкоди та продовжити з’єднання. Важливо, щоб ці дані були перевірені, щоб вони точно збіглися з тими, які надіслав пристрій. Наслідки для прийнятих змінених даних можуть бути як збій у телефонній розмові, так і катастрофічними, як електростанції, які отримують неправильні контрольні коди.

Доступність. Доступність − це третя частина тріади CIA. Цей принцип вимагає, щоб усі інформаційні системи були функціональними та завжди доступними. Це важлива мета, тому що без доступності ніщо інше не має значення. Якщо система недоступна, вона нікому не корисна. Коли ви маєте справу зі стільниковими мережами, область, яка не поширюється, може мати

серйозні наслідки. В нинішній час більшість користувачів не мають стаціонарних телефонів, а громадських телефонів дуже мало. Коли йдеться про безпеку життєдіяльності, а комунікація має вирішальне значення, система, яка забезпечує комунікації, є життєво важливою.

Розвиток розуміння критичної інфраструктури. При виборі критичності телекомунікаційних елементів, які повинні піддаватися особливій перевірці, основну увагу слід приділяти критичній інфраструктурі, яка визначається як:

– Державні мережі та центри обробки даних.

– Інфраструктура, яка використовується постачальниками основних продуктів і послуг: енергетика, продовольство, сировина, залізниці, аеропорти, телекомунікації, банки, інтернет-біржі, водоканали, лікарні.

– Інфраструктура критично важлива для високоцінних підприємств або має ключове стратегічне значення для економіки країни.

Необхідно розуміти, що критичність мереж і конкретних мережевих елементів повинна оцінюватися на основі (потенційно порушених) додатків, підтримуваних цими мережами. Навіть короткочасний збій в підключенні в обмеженій географічній зоні або вплив на вимоги до затримки для критично важливої послуги може призвести до смертельних наслідків. Таким чином, безперешкодний доступ до підключення стає таким же важливим, як і доступ до електрики.

Мережі 5G будуть засновані на хмарі, тобто їх інфраструктура буде складатися з взаємопов'язаних центрів обробки даних, або "хмар". Вони забезпечують середовище віртуалізації, в якому мережеві функції виконуються як віртуальні мережеві функції в загальній інфраструктурі, що надає віртуалізовані обчислювальні, мережеві та запам'ятовуючі ресурси.

Центри обробки даних будуть з'єднані між собою транспортними мережами, що складаються з вузлів транспортної мережі (наприклад, оптичних комутаторів) і фактичних ліній зв'язку (наприклад, оптоволоконних мереж). Транспортні мережі також забезпечать взаємозв'язок між центрами обробки даних, що належать до різних мереж мобільного зв'язку, що полегшить роумінг і зв'язок між абонентами різних мереж.

Мобільний доступ (RAN) складається з антен, радіочастотного та широкосмугового обладнання. У 5G RAN може бути реалізований в різних топологіях, починаючи від "класичних" розподілених мереж, заснованих на специфічній функції фізичної мережі HW (PNF), до віртуалізованих архітектур (vRAN /VNF), заснованих на великій кількості Edge Cloud (граничних хмар). Edge Cloud не буде виділена для RAN, але також буде містити частину Ядра, в основному шлюзи, і додатки для реалізації варіантів використання з низькою затримкою, підтримуваних 5G. Ось чому різниця між мобільним доступом і ядром стає все більш розмитою.

Хоча пристрої, що використовують мережу, зазвичай не є активами операторів мобільного зв'язку, вони все одно можуть містити, відповідно до специфікацій 3GPP, захищене обладнання, зазвичай відоме як "SIM-карта", але в специфікаціях зване UICC (Universal Integrated Circuit Card). UICC знаходиться під контролем оператора мережі і містить дані і програмне

забезпечення, зване додатком USIM (Universal Subscriber Identity Module). Додаток USIM на UICC має важливе значення для безпечного зв'язку між пристроєм і мережею і може розглядатися як частина активів операторів мобільного зв'язку. Для пристроїв Інтернету речей UICC може бути вбудований, і тільки його частина USIM знаходиться під контролем оператора.

Таблиця 1. Класифікація критичності інфраструктурних активів 5G.

Функція 5G / мережевий елемент	*Класифікація*	*Коментар*
Центри обробки даних	Критична	- Центри обробки даних розміщують: критично важливі функції мережі 5G, конфіденційні мережеві і призначені для користувача дані, а також інтерфейси до інших мереж. - ближче до границі (DC) ризик може зменшитися, оскільки вплив успішних атак носить регіональний характер.
Транспортні мережі (вузли і лінії зв'язку, наприклад, оптичні комутатори і волокна; Комутатори SDN)	Висока	- фізичний вплив, можливе порушення роботи мережі, - загроза прослуховування може бути зменшена за допомогою шифрування, - резервування дозволяє долати атаки на окремі транспортні вузли та канали
Об'єкти IPX	Висока	- подібно до транспортних мереж, трафік може бути захищений за допомогою механізмів, зазначених у 3GPP, або механізмів, визначених іншими організаціями, такими як GSMA.
Невіртуалізовані базові станції	Середня	- Атаки зазвичай мають локальний вплив, можливо надмірне покриття з інших базових станцій, конфіденційні дані захищені в захищеному середовищі базової станції; однак впровадження DoS-атаки в ядро також представляє ризик
Антена	Низька	- Низький рівень впливу; тільки локалізовані DoS-атаки
UICC/USIM	Низька	- висока апаратна безпека, дуже локальний вплив при зломі або клонуванні USIM

Класифікація критичності заснована на географічному охопленні/кількості абонентів, які постраждали в разі збою [3]. Однак фактичний рівень ризику залежить від програм, які можуть бути скомпрометовані.

Література

1. R. Piqueras Jover and V. Marojevic. “Security and Protocol Exploit Analysis of the 5G Specifications”. In: IEEE Access 7 (2019), 24956–24963. ISSN: 2169-3536. doi: 10.1109/ACCESS.2019.2899254.
2. Kim Zetter et al. Florida Cops’ Secret Weapon: Warrantless Cellphone Tracking. 2014. URL: https://www.wired.com/2014/03/stingray/.
3. Nokia. 5G Security Risks and Mitigation Measures. URL: https://www.nokia.com/sites/default/files/2021-05/Whitepaper-5G-security-Nokia-STC-March-31-2021.pdf.

УДК 621.382

ПРОГРАМА ОЦІНКИ ЗВ'ЯЗНОСТІ ВУЗЛІВ БЕЗПРОВОДОВИХ ЕПІЗОДИЧНИХ МЕРЕЖ ПРИ УМОВІ ЗАСТОСУВАННЯ БПЛА

Сушин І.О., Лисенко О.І.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: rubin268@ukr.net

THE PROGRAM FOR ASSESSING THE CONNECTIVITY OF NODES OF WIRELESS EPISODIC NETWORKS UNDER THE CONDITION OF USING UAVs

The article describes the main problems of the duration of connectivity of mobile subscribers (nodes) (MA) of a wireless episodic network (BEM consisting of MA and UAV) in conditions of direct radio visibility and taking into account relaying. The obtained results can be used in the UAV network topology control method.

Зв'язність пари вузлів визначається характеристиками різних рівнів інформаційної взаємодії OSI, такими як дальність радіозв'язку, пропускна здатність каналів, затримка передачі інформації та ін. В даному розділі пропонується розрахунок зазначених характеристик та їх аналіз в залежності від системних параметрів мережі.

Безпроводова епізодична мережа передачі даних зазвичай функціонує у межах прямої радіо видимості вузлів. При чому слід розрізняти пряму геометричну видимість та пряму радіо видимість (*line of site, LOS*), що передбачає наявність не лише прямої геометричної видимості, а й вільної першої зони Френеля, у якій розповсюджується основна енергія радіосигналу [2, ст. 214].

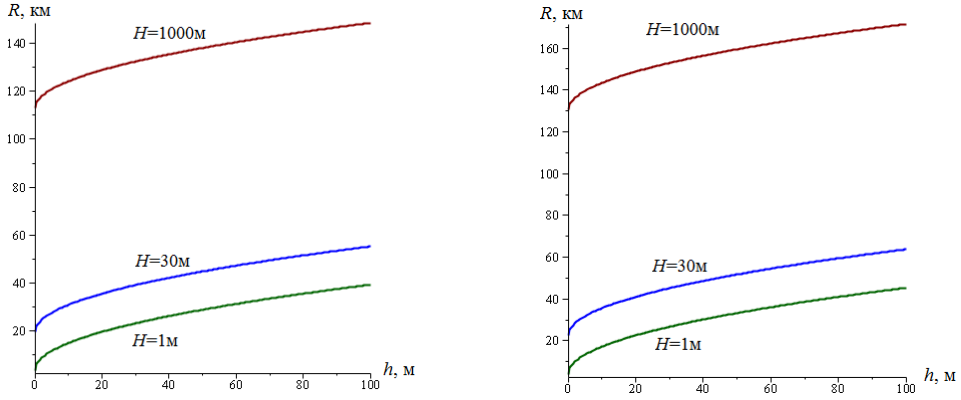
При роботі на рівнинній поверхні Землі радіус зони прямої (геометричної) видимості (R, км) визначається висотами розміщення передавальної (H, м) та приймальної (h, м) антени [Гавриленко]: $R = 3{,}57(\sqrt{KH} + \sqrt{Kh})$, де K – поправочний коефіцієнт, що враховує рефракцію радіохвиль.

На рис.1 приведені радіуси прямої видимості при K=1 (а) та K=4/3 (б).

Із графіків видно, що типове значення геометричної видимості пари абонентів (пішоходів), що знаходяться на рівнинній місцевості, в ідеалі може становити 7-10 км. У той час як дальність прямої видимості між пішоходом та БПЛА сягає понад 130 км.

Основними характеристиками, що визначають ефективність функціонування протоколу множинного доступу (МД) до загального канального ресурсу, є : середня швидкість передачі, середня затримка передачі та граничне значення трафіку, при якому досягається межа стійкої

роботи мережі (МС). Ці параметри визначаються як функція системних параметрів, серед яких основними є інтенсивність трафіку, швидкість передачі, довжина пакету, геометричні розміри мережі або узагальнюючий їх інтервал уразливості [3].



а) б)

Рис. 1. Дальність прямої видимості з урахуванням висоти підвісу антен при різних поправочних коефіцієнтах: *K*=1 (а) та *K*=4/3 (б).

Середня швидкість передачі представляє собою математичне очікування випадкової величини, що визначає кількість безконфліктно переданих пакетів за одиницю часу. В даній роботі за одиницю часу прийнято час передачі самого пакету *T*, тоді максимальним теоретичним значенням середньої швидкості передачі буде одиниця. Максимальне значення середньої швидкості передачі у літературі часто називають *пропускною здатністю* (іноді – ємністю) протоколу МД.

Середня затримка передачі – це нормований інтервал часу (в одиницях тривалості передачі пакету *T*) з моменту появи на вході вузла запиту на передачу до завершення безконфліктної передачі пакету даних. При чому враховується тільки два фактори, що перешкоджають передачі: затримка доступу, тобто час до моменту отримання дозволу на передачу, та затримка повторної передачі, що зумовлена лише пошкодженням пакетів при їх інтерференції. Дана характеристика розраховується у наступному підрозділі.

Граничне значення трафіку характеризує область застосування протоколу МД у конкретних умовах, а також визначає кількість вузлів у зоні дії МА та БПЛА, що визначається також у подальших підрозділах.[3]

Для аналізу вище вказаних характеристик та визначення їх потенційно можливих значень будемо використовувати аналітичні моделі, що будуються із використанням елементів теорії відновлення та припущення, що кількість абонентів нескінченно велика, кожен з яких генерує пакети з нескінченно малою швидкістю. Останнє є фактично припущенням про пуасонівський характер процесу надходження пакетів для передачі по радіоканалу. При цьому інтенсивність надходження пакетів вимірюється кількістю за час передачі пакету *T* та позначається буквою *G*. Середня швидкість передачі *S* також вимірюється в кількості пакетів за час *T*, але що передані безконфліктно. Припускається також, що всі пакети мають однакову

довжину L. Данні моделі оперують із середніми значеннями часових відрізків стану радіоканалу. Також будемо вважати, що службові пакети (квитанції), що підтверджують вдалий прийом пакету даних, мають нормовану довжину та передаються по окремому каналу безконфліктно.

Під інтенсивністю G надходження пакетів на передачу, що була вказана раніше, будемо розуміти сумарну інтенсивність, що включає як вхідний потік первинних пакетів Z_1, так і потік пакетів Z_2, що передаються повторно. Потік Z_1 кожного вузла формують як власні пакети, так ті, що потрібно ретранслювати від інших вузлів (визначаються згідно заданої матриці тяжіння Γ), а потік Z_2 визначаються процедурними характеристиками протоколу МД та значеннями його системних параметрів, а саме інтервалом часу перед повторною передачею. На практиці для стійкої роботи мережі інтенсивність поточного трафіку не має перевищувати $0{,}8g$, де g – поріг стійкості, що визначається типом протоколу МД .

На практиці зазвичай для взаємодії МА на канальному рівні використовують протокол випадкового множинного доступу із контролем несучої (МДКН). Для нашого випадку оберемо гнучку стратегію МДКН, тоді згідно середню швидкість передачі можна визначити за наступною формулою:

$$S = \frac{G\exp(-aG)}{G(1+2a)+\exp(-aG)}, \qquad (1)$$

де a – нормований максимальний час розповсюдження радіосигналу в мережі.

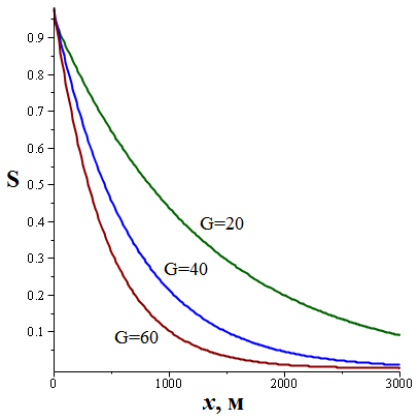


Рис. 2. Графіки залежності ПЗ каналу МА-МА від відстані між вузлами при різних значеннях інтенсивності трафіку.

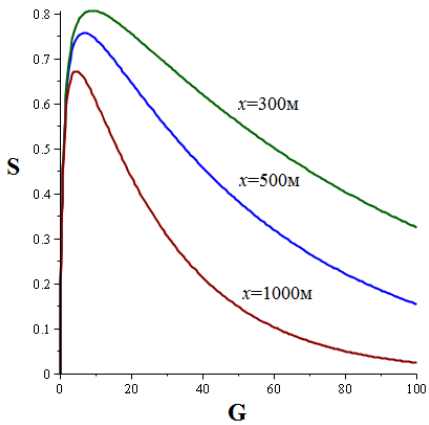


Рис. 3. Графіки залежності ПЗ каналу МА-МА від інтенсивності трафіку при різних значеннях відстані між вузлами.

Враховуючи, що $a = \frac{x \cdot V}{c \cdot L}$, де x – максимальна відстань між ретранслятором і абонентом (тобто між МА), м; c – швидкість розповсюдження сигналу, м/с; L – довжина пакету, біт; V – швидкість передачі, біт/с, та підставляючи (17) в (16) отримаємо:

$$S = \frac{G \cdot \exp(-\frac{x \cdot V}{c \cdot L} G)}{G(1 + 2\frac{x \cdot V}{c \cdot L}) + \exp(-\frac{x \cdot V}{c \cdot L} G)} \qquad (2)$$

Підставляючи наступні вихідні дані: V=11Мбіт/с, c=3*10^{8}м/с, L=1000біт у вираз (1), матимемо наступні графіки залежності S на канальному рівні МА-МА (рис.2, 3, 4).

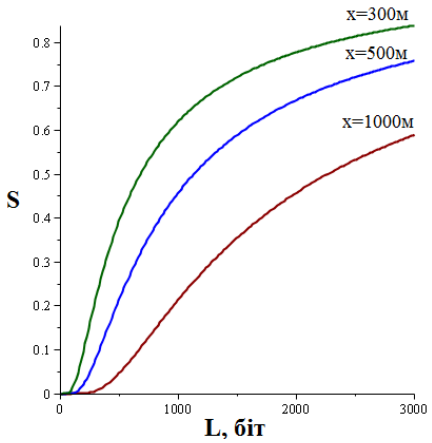


Рис. 4. Графіки залежності ПЗ каналу МА-МА від довжини пакету при різних значеннях відстані між вузлами (при *G*=40).

Аналізуючи графіки на рис.2, можемо бачити, що середня швидкість передачі монотонно спадає при збільшенні максимальної відстані між вузлами x. Це пов'язано з тим, що при збільшенні x зростає зона уразливості a, що спричиняє ріст кількості колізій при організації МД. Також згідно рис.3 збільшення x призводить до зменшення межі стійкості g та діапазону стійкої роботи протоколу МД. Так при x=300м (a=0,011) g становить приблизно 9 ($S_{max} \approx 0{,}81$), при x=500м (a=0,0183) g≈6,8 ($S_{max} \approx 0{,}76$), а при x=1000м (a=0,0366) g≈4,6 ($S_{max} \approx 0{,}67$). Проблему збільшення пропускної здатності при заданому x (або ж еквівалентно збільшення максимальної відстані між МА x при заданій S) можна вирішити шляхом збільшення довжини пакету L, однак при цьому зростає ймовірність ураження пакета завадою та час доставки пакетів в мережі. Також цю проблему можна вирішити шляхом зменшення швидкості передачі V (тобто виділеної частотної смуги Π), але це – нераціонально, оскільки при цьому знижають інші основні характеристики мережі – пропускна здатність та коефіцієнт використання смуги частот. Отже, вибір максимальної відстані між вузлами (радіусу радіо покриття МА) x визначається мінімальним допустимим значенням пропускної здатності

протоколу МД при заданих V та L.[3]

Організація інформаційної взаємодії на мережному рівні між будь-якою парою абонентів мережі потребує наявності маршруту передачі даних заданої якості (QoS). Критерієм якості або метрикою маршруту (наприклад, при передачі голосового трафіку) може виступати кількість ретрансляцій або ж величина затримки передачі пакету із кінця в кінець через мережу проміжних вузлів-ретрансляторів. У загальному вигляді ця величина матиме наступний вигляд: $D = T_{пак} + T_{дост} + T_{росп} + T_{обр} + T_{буф}$, де $T_{пак}$ – час пакетизації (формування пакету у вузлі-відправнику), що залежить від типу трафіку (алгоритму формування пакету, наприклад, для голосу – від типу кодеку); $T_{дост}$ – середній час затримки доступу до каналу (для випадкового МД), що залежить від інтенсивності трафіку та пропускної спроможності каналу; $T_{росп}$ – час розповсюдження сигналу в середовищі передачі (не залежить від типу трафіка); $T_{обр}$ – час обробки пакету в проміжних вузлах мережі (залежить від типу трафіку); $T_{буф}$ – час затримки у буфері проміжних вузлах мережі (залежить від типу трафіку, дисципліни обслуговування, пріоритетності трафіку (SLA)). Для пакету IP середньої довжини 576 біт та при швидкості кодування 64кбіт/с час пакетизації становитиме 9 мс, чим можна знехтувати при грубій оцінці затримки передачі. Час обробки пакету в проміжних вузлах мережі також будемо вважати несуттєвим. Також припустимо, що в мережі передається однорідний трафік, на проміжних вузлах застосовується дисципліна FIFO («перший прийшов, перший обслуговується»), при чому пакет в вузлі обробляється відразу без відправки його у чергу, тобто часом затримки в буфері можна знехтувати.[5, ст. 223]

Наведений розрахунок є наближеним через те, що окрім припущення щодо пуасонівського характеру потоку пакетів, було розглянуто середнє значення трафіку, генерованого усіма абонентами, що не завжди виконується на практиці. Не дивлячись на це, наведений розрахунок залишається справедливим при умові неперевищення усіма абонентами сумарної допустимої величини трафіку в мережі, що обмежується максимальною середньою затримкою передачі. Саме цей параметр, виміряний кожним абонентом мережі шляхом обліку часу отримання квитанцій на ряд переданих пакетів, може служити обмеженням на генерований їм трафік або визначати момент переключення передачі пакетів з мережі МА на мережу БПЛА та навпаки. Знаючи кількість наземних абонентів, їх координати та трафік створюваний ними, БПЛА може знайти своє оптимальне розміщення у просторі, що дасть змогу не тільки забезпечити геометричну зв’язність абонентів, а й підвищити інформаційні характеристики мережі (такі як пропускна здатність) завдяки з’єднання віддалених абонентів та розвантаження перевантажених каналів в районах скупчення абонентів.

Висновки. 1. Максимальна дальності зв’язку (діапазону УКВ) обмежується кривизною земної поверхні та висотами підвісу передавальної та прийомної антени. Так, з урахуванням рефракції, максимальна протяжність радіолінії МА-МА може становити 7-10 км, а БПЛА-МА –

більше 130км при висоті баражування БПЛА більше 1км. Крім того, максимальна дальність радіозв'язку обмежується енергетикою радіолінії, при якій відношення сигнал-шум в точці прийому не менше визначеної величини для забезпечення заданої ймовірності бітової помилки (BER) при заданому виді модуляції (відповідній швидкості передачі). Так при застосуванні типового обладнання 802.11a/b/g максимальна протяжність радіолінії МА-МА не перевищує 1000м (на швидкості передачі 1Мбіт/с), а при реальному рельєфі місцевості – не більше 630м (для великого міста).

2. При необхідності передачі інформації на більші відстані, аніж дальність прямого з'єднання, необхідно застосовувати механізм ретрансляції (комутації) пакетів через проміжні вузли. Максимальна дальність зв'язку у даному випадку визначається заданою величиною затримки передачі «із кінця в кінець» для забезпечення необхідної QoS. Так для застосувань реального часу (VoIP, відеоконференції і т.п.) кількість ретрансляцій мережею БПЛА не має перевищувати 6-ти, а для застосувань не критичних до затримки (короткі трансакції, масиви даних, потокове відео і т.п.) може становити декілька десятків при заданій інтенсивності трафіку. Також показано, що при двічі більшій інтенсивності трафіку середня затримка передачі ланки БПЛА-БПЛА втричі переважає середню затримку передачі на ланці МА-МА. Отже при кількості ланок у маршруті мережі МА більше ніж 3 доцільніше передавати інформацію через мережу БПЛА при наявності покриття останньої.

Література

1. Lysenko O. I. Optimal control of telecommunication aeroplatform in the area of emergency / O. I. Lysenko, S. V. Valuiskyi, P. I. Kirchu, A. V. Romaniuk // Telecommunication sciences. - 2013. - Vol. 4, no. 1. - С. 14-20. - Режим доступу: http://nbuv.gov.ua/UJRN/Telnau_2013_4_1_5.
2. S. Valuiskyi, A. Lysenko, T. Pryshchepa and S. Chumachenko, "The problem of finding a rational topology of wireless sensor networks using UAVs," 2015 Second International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), 2015, pp. 213-215, doi: 10.1109/INFOCOMMST.2015.7357316.
3. Lysenko O., Romaniuk V., Tachinina O., Valuiskyi S. (2020) The Problems of Control in Wireless Sensor and Mobile Ad-Hoc Networks. In: Nechyporuk M., Pavlikov V., Kritskiy D. (eds) Integrated Computer Technologies in Mechanical Engineering. Advances in Intelligent Systems and Computing, vol 1113. Springer, Cham. https://doi.org/10.1007/978-3-030-37618-5_33.
4. Ming Zhu, Fei Liu, Zhiping Cai, Ming Xu, "Maintaining Connectivity of MANETs through Multiple Unmanned Aerial Vehicles", Mathematical Problems in Engineering, vol. 2015, Article ID 952069, 14 pages, 2015. https://doi.org/10.1155/2015/952069.
5. Бунин С. Г. Вычислительные сети с пакетной радиосвязью / С. Г. Бунин, А. П. Войтер. – К.: Техника, 1989. – 223 с.
6. Ильченко М. Е. Сотовые радиосети с коммутацией пакетов / М. Е.Ильченко, С. Г.Бунин, А. П.Войтер. – К.: Наукова думка, 2003. – 266 с.

УДК 621.396

ПРОГРАМНО-КОНФІГУРОВАНА СУПУТНИКОВА ІНФРАСТРУКТУРА ІНТЕРНЕТУ РЕЧЕЙ

[1]Жабчик А.І., [1]Нарушкевич О.М., [1]Наритник Т.М., [2]Капштик С.В.
[1]*Навчально-науковий інститут телекомунікаційних, систем КПІ ім. Ігоря Сікорського, Україна*
[2]*Національний центр управління та випробувань космічних засобів, Україна*
E-mail: nastia2767@gmail.com; sashanarushkevych@gmail.com; director@mitris.com; s.kapshtyk@spacecenter.gov.ua

SOFTWARE-CONFIGURED SATELLITE INFRASTRUCTURE OF THE INTERNET OF THINGS

Abstract. The state of use of the satellite component for Internet of Things systems operating on the basis of the 5G ecosystem is considered. A multi-level satellite infrastructure is proposed, which is designed to support the functioning of Internet of Things systems and includes geostationary and low-orbital components. To support Internet of Things systems, the satellite infrastructure includes computing power for the implementation of cloud, fog, and edge computing. In order to improve data transmission management, it is proposed to create a software-configured data transmission network as part of the satellite infrastructure of the Internet of Things. The data transmission network combines geostationary and low-orbit components. The use of software-configured data transmission network technology makes it possible to simplify the operational adjustment of the low-orbit component to the regional characteristics of Internet of Things services and generated traffic.

Інтернет речей став одним з основних драйверів розвитку телекомунікаційних систем. Впровадження систем Інтернету речей супроводжується постійним зростання попиту на вільну пропускну здатність телекомунікаційних мереж. З цієї причини в специфікаціях стандартів 4G та 5G дослідницька група 3GPP починаючи в релізу 14 виділяє системи і послуги Інтернету речей в окремий напрямок, який формалізований у вигляді вузькосмугової послуги Інтернету речей (англ. 5GLTENarrowbandInternetofThings, або NB-IoT). Для розширення зони надання послуг 4G, 5G, включаючи послуги NB-IoT, дослідницька група 3GPP починаючи з релізу 14 включає до складу інфраструктури мобільної мережі супутникову складову. До беззаперечних переваг супутникових систем зв’язку та передачі даних відносяться практично глобальна зона обслуговування та спроможність забезпечити підключення незалежно від стану наземних телекомунікаційних мереж.В релізах групи 3GPP супутникова складова розглядається в першу чергу як оперативний засіб забезпечити підключення віддалених районів із непідготовленою інфраструктурою, де розміщені базові станції, до кореневої мережі. Для цього типу послуг група 3GPP ввела термін “неназемна мережа” (англ. Non-TerrestrialNetworks). У відповідь на пропозиції групи 3GPP розробники та оператори супутникових телекомунікаційних систем звернули особливу увагу на забезпечення сумісності цих систем із наземними системами широкосмугового доступу 5G.

В релізі 17 супутниковій компоненті відводиться більш важливе місце в екосистемі 5G [1], яка розглядається як критично важлива складова глобальної екосистеми 5G. В релізі визначені специфікації для безпосереднього підключення 5G до супутника (англ. direct-to-device 5Goversatellite). Реліз 17 передбачає використання геостаціонарної і низькоорбітальної складових, відзначаючи їх переваги та недоліки.В частині розвитку інфраструктури 5G супутникова компонента розглядається як засіб для підключення віддалених зон обслуговування для технології, що отримала назву «Нове радіо не

наземних мереж» (англ. NewRadio - Non-TerrestrialNetworks, NR-NTN). В цьому випадку NR-NTN можна розглядати як частину розширеної мобільної широкосмугової мережі (англ. EnhancedMobileBroadband, eMBB) [10]. Зважаючи на вимоги ринку щодо впровадження систем і послуг Інтернету речей ряд провідних супутникових компаній – операторів почали пропонувати на ринку власні рішення. На сьогодні більше 80% обсягу послуг супутникового Інтернету речей надають компанії Inmarsat, Iridium, GlobalStari ORBCOM [5].

Одним з головних напрямків розвитку супутникових телекомунікаційних систем є впровадження технології програмно-конфігурованих мереж (англ. Software-definedNetwork, SDN)[4]. Метою впровадження цієї технології є спрощення управління конфігурацією супутникової мережі та забезпечення її гнучкості, надійності, адаптації до нових видів послуг, тощо.

До особливостей супутникових систем, які передбачають надання послуг Інтернету речей, важливою властивістю є їх здатність забезпечити надання послуг із різними стандартами IoT, зокрема із стандартами, що базуються на технології LoRa® та на технології IoT-NTN. Для досягнення такої мети підхід, який базується на використання технологійSDN та програмно-конфігурованого радіо (Software-DefinedRadio, SDR), є привабливим і створює передумови для подальшої інтеграції до екосистеми 5G.На спрощення реконфігурації мережі та спільного використання її ресурсів багатьма споживачами послуг орієнтовані технології «віртуалізації мережевих функцій» (англ. NetworkFunctionVirtualization, NFV) та віртуалізації мережі (англ. NetworkVirtualization, NV) [11]. В якості перспективної супутникової телекомунікаційної системи, яка спрямована на надання послуг Інтернету речей із використанням власних обчислювальних потужностей для реалізації концепції краєвих (або граничних), туманних та хмарних обчислень, пропонується багаторівнева програмно-конфігурованасупутникова інфраструктура Інтернету речей.

Програмно-конфігурована супутникова інфраструктура Інтернету речей (далі - IoTсупутникова інфраструктура) складається з трьох основних сегментів:

- геостаціонарний сегмент;
- низькоорбітальний сегмент;
- наземний сегмент.

На рис.1. представлена архітектура космічної складової IoT супутникової інфраструктури. Геостаціонарний сегмент включає GEOсупутники-ретранслятори та GEO-супутники – хмарні центри даних. GEO супутники-ретранслятори призначені для забезпечення формування та підтримки ліній зв’язку типу «супутник-супутник» із LEO супутниками-ретрансляторами, для взаємодії із наземним комплексом управління та наземними засобами операторів і сервіс-провайдерів, а також із наземними мережами передачі даних.

GEOсупутники-ретранслятори обладнані цифровим корисним навантаженням, яке функціонує із використанням технологій SDN та SDR. В конструкції високочастотної частини корисного навантаження GEO супутників-ретрансляторів використовуються технології супутників великої пропускної здатності (англ. High-ThroughputSatellite, HTS), що дозволяє формувати одночасно велику кількість керованих та нерухомих променів. Керовані промені призначені для супроводження руху LEO супутників-ретрансляторів.

Для формування керованих променів використовуються фазовані антенні решітки. GEO супутники – хмарні центри даних призначені для оброки, збереження та поширення даних, та надання обчислювальної потужності для підтримки послуг Інтернету речей, побудованих із використанням «хмарної» складової.Усі GEO супутники об’єднані лініями зв’язку типу «супутник-супутник», що дозволяє сформувати ГСО мережу передачі даних кільцевої архітектури.

Низькоорбітальна складова IoT супутникової інфраструктури побудована на базі архітектури розподіленого супутника [12]. Розподілені супутники розташовані в кількох

орбітальних площинах на низькій навколоземній орбіті. Параметри орбіти, кількість орбітальних площин і розподілених супутників в кожній площині визначається зоною обслуговування та показниками безперервності обслуговування. Низькоорбітальна складова призначена для забезпечення взаємодії із кінцевими пристроями Інтернету речей в режимі безпосереднього доступу (англ. Direct-to-Satellite) та із використанням терміналів кінцевих споживачів. Режим безпосереднього доступу використовується для послуг Інтернету речей на базі вузькосмуговихпротоколів LoRa® та NB-IoT. При використанні послуг Інтернету речей, які вимагають широкосмугового каналу, включаючи канали передачі відеоінформації, використовуються термінал користувачів, аналогом яких є термінали низькоорбітальних систем Starlinkта OneWeb.

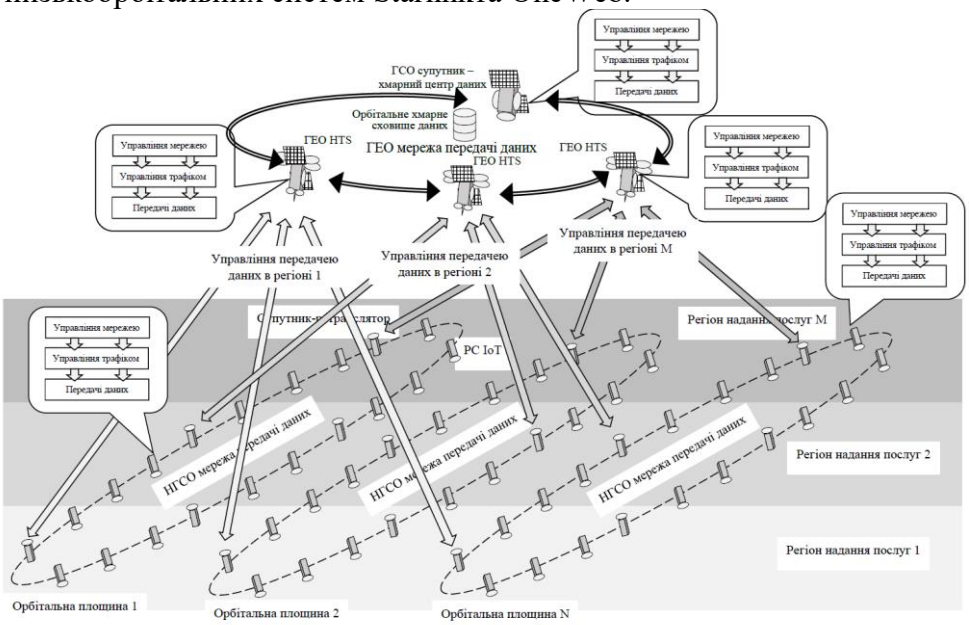


Рис.1. Архітектура космічної складової IoT супутникової інфраструктури.

Кожен розподілений супутник за допомогою ліній зв’язку типу «супутник-супутник» встановлює лінії зв’язку з двома сусідніми розподіленими супутникам в своїй орбітальній площині та по одному розподіленому супутнику в двох сусідніх орбітальних площинах. Лінії зв’язку між розподіленими супутниками утворюють транспортну мережу для орбітальної системи передачі даних низькоорбітальної складової IoT супутникової інфраструктури. Для забезпечення повнозв’язностиIoT супутникової інфраструктури до складу кожної орбітальної площини низькоорбітальної складової введені LEO супутники-ретранслятори, завданням яких є підтримка лінії «супутник-супутник» з GEO супутниками-ретрансляторами.

До особливостей низькоорбітальної складової відносяться фактори, які зумовлені особливостями низької навколоземної орбіти. А саме, супутники постійно рухаються відносно об’єктів, розташованих на поверхні Землі, та відносно супутників, розташованих на геостаціонарній орбіті. Тому зона радіобачення низькоорбітального супутника постійно рухається по поверхні Землі, проходячи усі широти в межах зони обслуговування системи, а склад низькоорбітальних супутників, які знаходяться в межах до зони радіобачення геостаціонарного супутника, постійно змінюється. Зважаючи на певні відмінності в складі та специфіці послуг Інтернету речей в різних регіонах світу, необхідно зазначити, що зони обслуговування супутників усіх орбітальних площин зі складу низькоорбітальної складової в певний час будуть проходити по усіх регіонах поверхні Землі. Тому в складі низькоорбітальної складової можна виділити певні групи супутників в кожній орбітальній площині, які надають послуги у визначених регіонах світу, і таким чином розділити склад супутників кожної орбітальної площини на певні групи, як це показано на рис.1. Супутники зі складу геостаціонарної складової

знаходяться в стаціонарному положенні відносно цих регіонів. Тому ці супутники мають забезпечувати підтримку функціонування низькоорбітальної складової і надання нею послуг Інтернету речей згідно регіональної специфіки, зважаючи на постійну зміну складу супутників низькоорбітальної складової у визначеному регіоні. Така відмінність враховує не тільки алгоритми обробки інформації Інтернету речей, а й маршрутизацію циркулюючої інформації.

IoT супутникова інфраструктура має власні обчислювальні потужності, які реалізують хмарні, туманні та краєві, або граничні обчислення, що відповідає багаторівневій ієрархічній архітектурі систем Інтернету речей. Хмарні обчислення реалізуються обчислювальними потужностями спеціально виділених GEO супутників – хмарних центрів обробки даних. Для реалізації туманних і краєвих (граничних) обчислень до розподілених супутників зі складу низькоорбітальної складової введені супутники-обчислювачі [12].

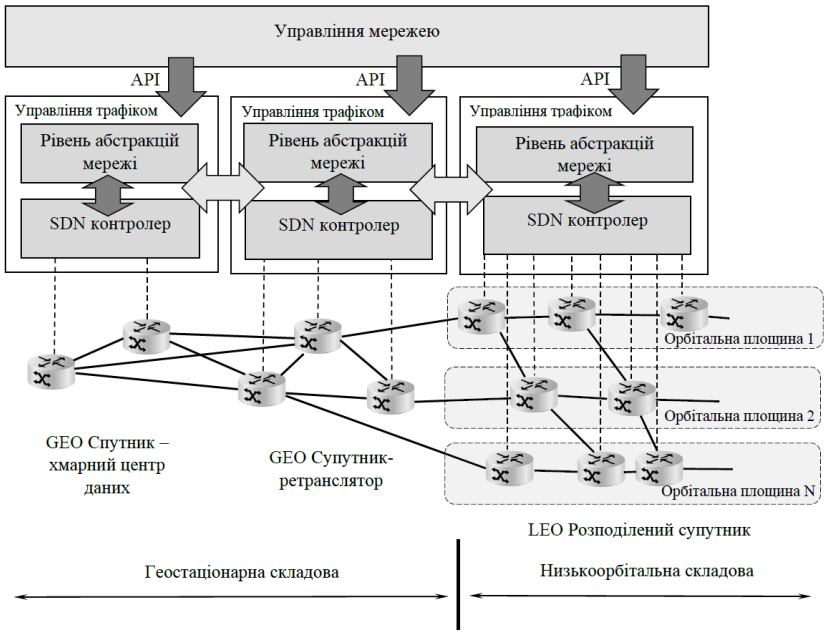


Рис.2. Архітектура SDN мережі IoT супутникової інфраструктури.

Геостаціонарна та низькоорбітальна складові IoT супутникової інфраструктури утворюють єдину SDN мережу передачі даних. На рис.2 представлена SDN мережа передачі даних IoT супутникової інфраструктури. Функціонал управління передачею даних ГСО мережі розподілений між трьома площинами (див. рис.2): управління мережею, управління трафіком та передачі даних. На рівні управління мережею здійснюється управління архітектурою IoTсупутникової інфраструктури як мережі передачі даних в цілому та її складових для надання послуг Інтернету речей. Для спрощення управління мережею використовуються технології NFV та NVв поєднанні із гіпервізорами, як засобами віртуалізації функцій і спрощення представлення інформації в графічному вигляді. Рівень управління мережею здійснює управління геостаціонарною складовою і низькоорбітальною складовимиIoT супутникової інфраструктури. Рівень управління мережею взаємодіє із рівнем управління трафіком за допомогою програмованого інтерфейсу додатків (англ. ApplicationProgrammingInterface, API).

У відповідності до абстракцій мережі (англ. NetworkAbstractions), які визначені на підставі отриманих по північному інтерфейсу API, рівень управління трафіком визначає конфігурацію SDN контролерів ГЕО мережі передачі даних. Керуюча інформація у вигляді API через південний інтерфейс рівня управління трафіком доводиться до пристроїв рівня передачі даних, які здійснюють маршрутизацію інформації Інтернету речей, що циркулює в системі. Кожен із GEO супутників-ретрансляторів забезпечує інформаційних обмін із LEOсупутниками-ретрансляторами зі складу низькоорбітальної

складової в межах власної зони обслуговування. По каналу передачі даних, який побудований із використанням ліній «супутник-супутник» передаються дані слайсу даних Інтернету речей та інформація слайсу управління мережею передачі даних. На рис.2 показані західний і східний інтерфейси площини управління трафіком, які забезпечують передачі API між геостаціонарною та низькоорбітальною складовими.

У складі низькоорбітальної складової на базі ліній «супутник-супутник» між розподіленими супутниками сформовано низькоорбітальну SDNмережу передачі даних, яка є складовою частиною SDNмережі IoT супутникової інфраструктури. SDNконтролери зі складу рівня управління трафіком визначають розподіл потоків даних в межах низькоорбітальної складової та між низькоорбітальною та геостаціонарною складовими. Зважаючи на особливість руху низькоорбітальної складової відносно поверхні Землі перелік завдань, що реалізуються SDN контролерами динамічно змінюється у відповідності із рухом зони обслуговування розподіленого супутника відносно поверхні Землі. Зміна завдань здійснюється із використанням західного та східного інтерфейсів у відповідності до структур послуг Інтернету речей, які визначені API по північному інтерфейсу.

Висновки.

1. Розвиток сучасних телекомунікаційних мереж 4G, 5G передбачає використання геостаціонарної та низькоорбітальної супутникової складової для розширення зони обслуговування наземних мереж за технологією не наземних мереж NTN, і забезпечення підключення пристроїв Інтернету речей безпосередньо до супутника за вузькосмуговою технологією IoT-NB.
2. Для розвитку систем Інтернету речей запропонована багаторівнева супутникова інфраструктура, архітектура якої передбачає використання геостаціонарної і низької навколоземної орбіти, що відповідає концепції «не наземних мереж» екосистеми 5G.
3. Супутникова інфраструктура Інтернету речей має власні обчислювальні потужності для підтримки систем Інтернету речей, які побудовані за багаторівневою ієрархічною архітектурою, і реалізує хмарні обчислення на рівні геостаціонарної складової та туманні і краєві (граничні) обчислення на рівні низькоорбітальної складової.
4. Для організації передачі даних в супутниковій інфраструктурі Інтернету речей реалізована програмно-конфігурована мережа передачі даних, яка об’єднує геостаціонарну і низькоорбітальну складові. Використання технології програмно-конфігурованих мереж передачі даних дозволяє спростити управління системою передачі даних, її реконфігурацію та відновлення працездатності, і оперативно впроваджувати нові послуги Інтернету речей шляхом розробки програмованих інтерфейсів додатків.

Література

1. 3GPP реліз 17.
2. 5G from Space: An Overview of 3GPPNon-Terrestrial Networks / Xingqin Lin, Stefan Rommer, Sebastian Euler, Emre A. Yavuz, and Robert S. Karlsson
3. Softwaredefinedintelligentsatellite-terrestrialintegratednetworks:insightsandchallenges / ShuoYuan, MugenPeng, YaohuaSun, XiqingLiu / Digital Communications and Networks / Available online 21 June 2022 / https://doi.org/10.1016/j.dcan.2022.06.009
4. Inmarsat and hiSky Complete Test for IoT Service Offering / електронний документ. Режим доступу: https://www.satellitetoday.com/technology/2022/07/06/inmarsat-and-hisky-complete-tests-for-iot-service-offering/
5. Software-DefinedNext-GenerationSatelliteNetworks: Architecture, Challenges,andSolutions / Shuang Xu, Xing-Wei Wang, and Min Huang / 2169-3536 © 2018 IEEE, Vol.6, 2018, pp.4027-4041.
6. ІльченкоМ.Ю. Низькоорбітальна супутникова система інтернету речей на базі розподіленого супутника / М.Ю. Ільченко, Т.М. Наритник, В.І. Присяжний, С.В. Капштик, С.А. Матівєнко / Космічна наука і технологія. 2020. Т. 26. № 4, с. 57-85 / https://doi.org/10.15407/knit2020.04.000.

УДК 621.396

ВПРОВАДЖЕННЯ ЗАГАЛЬНИХ ПРИНЦИПІВ «STEM-ОСВІТИ» В НАВЧАЛЬНО-НАУКОВОМУ ІНСТИТУТІ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ КПІ ІМ. ІГОРЯ СІКОРСЬКОГО

Ільченко М.Ю., Якорнов Є.А.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: yakornovits@gmail.com

IMPLEMENTATION OF GENERAL PRINCIPLES OF "STEM EDUCATION" IN THE EDUCATIONAL AND SCIENTIFIC INSTITUTE OF TELECOMMUNICATION SYSTEMS, IGOR SIKORSKY KYIV POLYTECHNIC INSTITUTE

A brief comparative analysis of the education of students at the Educational and Scientific Institute of Telecommunication Systems of NTUU "KPI" was conducted for compliance with the general principles of the global trend of "STEM education" and the main problems of its implementation in Ukraine were shown. A brief comparative analysis of the education of students at the Educational and Scientific Institute of Telecommunication Systems of NTUU "KPI" was conducted for compliance with the general principles of the global trend of "STEM education" and the main problems of its implementation in Ukraine were shown.

В останні рокі в світі і в Україні [1,2] навчання молоді ведеться на основі використання базових принципів тренду «STEM» (англ. Science, Technology, Engineering, Mathematics), якій був введений National Science Foundation США та впроваджений у освітні програми навчальних закладів на національному рівні з метою розвитку та підсилення компетенцій учнів та студентів у науково-технічному напрямі для підготовки фахівців в галузях високих технологій к яким відносяться і інфокомунікації.

Ці загальні принципі включають:

- інтегровану освіту (проектний і міждисциплінарний підхід);
- удосконалення когнітивних навичок;
- активну участь студентів у навчально-практичній діяльності, (командна співпраця);
- розвиток критичного та креативного мислення, вміння працювати самостійно й у колективі;
- використання отриманих знань в реальному житті (реально виконані дослідні проекти).

Це додатково дає підсилення соціально-емоційної складової навчання та можливості широкого обсягу вибору професій та кар’єрного зростання у майбутньому, у тому числі і відкриття випускниками закладів вищої освіті (ЗВО) власних фірм.

Розглянемо коротко систему підготовки випускників Навчально-наукового інституту телекомунікаційних систем НТУУ «КПІ» (НН ІТС) та їх відповідність тренду «STEM».

З часу утворення кафедри засобів телекомунікацій у 1993 року та НН ІТС в 2002 році колишні школярі потрапляли в атмосферу взаємної поваги та доброзичливості у стосунках між студентами та викладачами. Завдяки високому професіоналізму викладачів зазначена атмосфера і сьогодні сприяє створенню умов для якісного навчання та наукового зростання молоді. Починаючи з дня першокурсника і до самого випуску студенти НН ІТС знаходяться в середовищі (рис. 1), що має за мету готувати висококваліфікованих, конкурентоспроможних, креативних, культурно освічених фахівців для галузі інфокомунікацій.

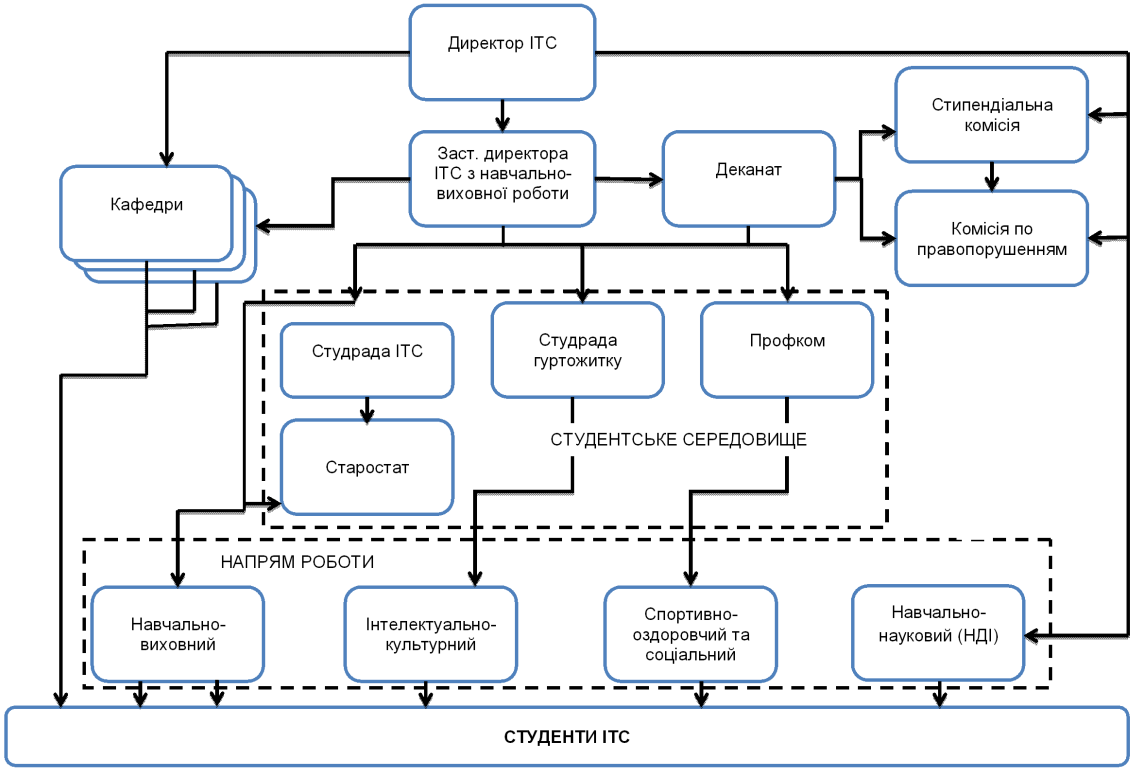


Рис. 1.

При цьому велика увага приділяється першій складовій абревіатури «STEM» - науки. Залучення окремих студентів до наукової роботи починається з другого курсу, четвертому сягає 70%, а на другому (магістерському) рівні підготовки практично всі студенти зобов'язані апробувати свої результати на різних наукових конференціях та оформити їх у вигляді статті чи патенту.

Деякі результати цієї роботи за останні рокі видні з діаграм на рисунки 2, на яких перший стовпчик показує кількість студентів, які беруть участь у науково – дослідної роботі (НДР), а це щорічно становить приблизно чверть від усього контингенту ІТС, другий - загальну кількість публікацій у виді тез на міжнародних конференціях, звітів з НДР, статей та патентів, у яких студенти публікуються разом із керівниками чи самі, а третій стовпчик – кількість учасників в Міжнародної науково-технічної конференції студентів та аспірантів «Перспективи розвитку інформаційно - телекомунікаційних технологій та систем» (ПРІТС), яка проводиться у НТУУ "КПІ" ім. Ігоря Сікорського на базі ІТС і де вони беруть участь особисто.

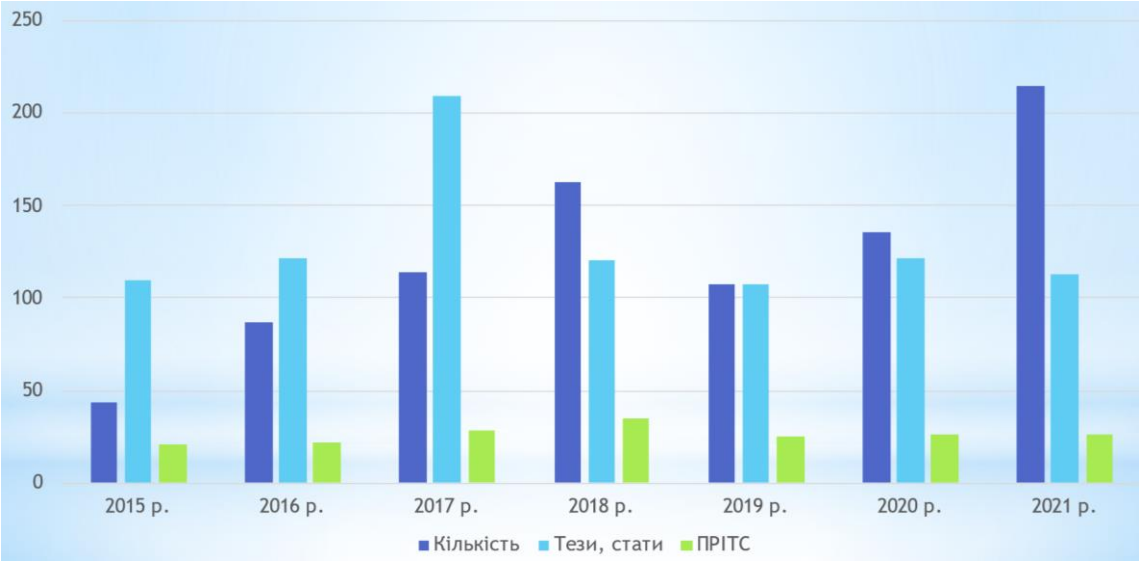


Рис. 2.

Участь студентів ІТС в НДР дозволяє почуватися впевнено і в інших аспектах тренду «STEM» технологічному (Technology) та інженерному (Engineering). Проявом цього є кількісні показники (рис. 3) участі у Всеукраїнських олімпіадах (за останні 15 років 19 студентів ІТС отримали 1-3 місця особисто та 57 – в командному заліку) та конкурсах студентських наукових праць інфокомунікаційного профілю (24 диплома 1-3 ступеня), а також різноманітних технологічно-інженерних конкурсах відомих в Україні телекомунікаційних фірм, наприклад, МТС (VODAFONE) «Професіонали майбутнього», та конкурсних стажувань у цих фірмах.

Рис. 3.

Сюди же можна віднести активну участь студентів ІТС у конкурсному відборі найкращих 10 студентів з України інфокомунікаційного напрямку підготовки на стажування у компанії «Хуавей» по програми «Насіння для майбутнего» на території Китаю. К ним відносяться наші кращі студенті, наприклад, Дарья Гордеева (2016 р.), Наталія Гвоздецька (2017 р.), Микита

Осокін (2018 р.) та інш.

Також викладачами ІТС постійно ведеться робота з підготовки найкращих студентів з доповідями про їх напрацювання на різних міжнародних форумах.

Що ж до четвертої компоненти тренду «STEM» - Mathematics, то по-перше, сам курс математики узгоджено з інфокомунікаційним профілем підготовки студентів, а по-друге, для першого та старших курсів в НН ІТС щорічно проводяться математичні олімпіади з подальшою участю переможців в олімпіадах на рівні університету.

Загалом така підготовка студентів ІТС забезпечує нашу державу висококваліфікованими спеціалістами (за останні 3 роки найвищі показники рекомендованих МОНУ абітурентів для вступу на 1й курс на денну форму навчання за держзамовленням до ІТС за спеціальністю 172 серед усіх ЗВО: 2020 р. -160, 2021 р. -180, 2022 р. -див. табл.), відкриває нашим найкращим випускникам дорогу як мінімум до Європейського союзу завдяки програмі двох дипломів з Технічним університетом Дрездена (за 15 років участь у програми більш 30 студентів ІТС) та забезпечує зміну поколінь викладачів у самому інституті (захист випускниками 17 кандидатських дисертацій та одної докторської в КПІ, 3 – х докторів філософії в Вестмінстерському університети (Лондон) та 2 – х в Дрездене).

Таблиця 1.

172 Телекомунікації та радіотехніка											
Факультет/ Університет	Ліцензія	Макс. обсяг держзамовлення	Дата та час	Пріоритет (Б+К), Денна						Загалом	Рекомендовано до зарахування за держзамовленням
				1	2	3	4	5	К-т		
НН ІТС	200	180	23.08.2022, 18-00	104	90	94	75	82	39	484	180
РТФ	130	125		74	64	52	53	27	17	287	102
ФЕЛ	55	55		18	20	27	24	17	13	119	25
ДУТ	150	124		53	58	44	35	43	14	247	109
Львівська політехніка	410	131		57	57	62	49	80	13	318	131
НАУ	550	69		18	25	36	39	33	20	171	42
	34	12		0	8	5	2	10	2	27	5
ХНУРЕ	50	17		13	17	9	3	8	2	52	17
	143	40		9	8	11	16	10	0	54	20
	100	46		10	16	15	9	12	0	62	28
	320	10		4	2	3	2	2	1	14	4
	175	15		3	3	2	8	3	0	19	7
ДУІТЗ (ОНАЗ)	70	52		23	10	18	11	10	5	77	52
КНУ ім. Т. Г. Шевченка	50	30		19	19	27	15	14	17	111	30
	35	31		17	34	20	20	12	13	116	31

Тренд «STEM» також передбачає колективну роботу з вирішення тієї чи іншої наукової проблеми. Тому в ІТС склалися і продовжують передаватися від покоління до покоління сильні традиції студентського самоврядування:

- кураторство старших курсів над першим;
- проведення старшокурсниками консультацій для 1,2 курсів зі складних для студентів предметів;
- видання студентської газети;
- організація дозвілля студентів, особливо організація двічі на рік

спортивно-ігрових заходів «Open Air» (усього 22 до початку COVID-19) на природі для всього інституту із запрошенням викладачів;

- активну участь у спортивному житті університету та інших загальноуніверситетських заходах;
- волонтерство та охорона об'єктів інфраструктури університету в умовах війни.

Особливо слід зазначити наявність в студентської Ради ІТС сектору наукової роботи, який різко активізував свою роботу на початку війни у виді Студентського конструкторського бюро [3], основної метою якого є волонтерство та допомога ЗСУ, наприклад, участь у випробуваннях перших в Україні «Starlink» Ілона Маска у зоні бойових дій у Миколаївській області.

Однак використання переваг «STEM-освіти» в школі та ЗВО України стримується, на наш погляд, політико-економічною ситуацією в країні та вкрай недостатнім фінансуванням науки та освіти з боку держави загалом, стан якої в 2016 року відображено (рис. 4) у доповіді Максима Стріхи, присвяченій імплементації закону України «Про наукову і науково-технічну діяльність».

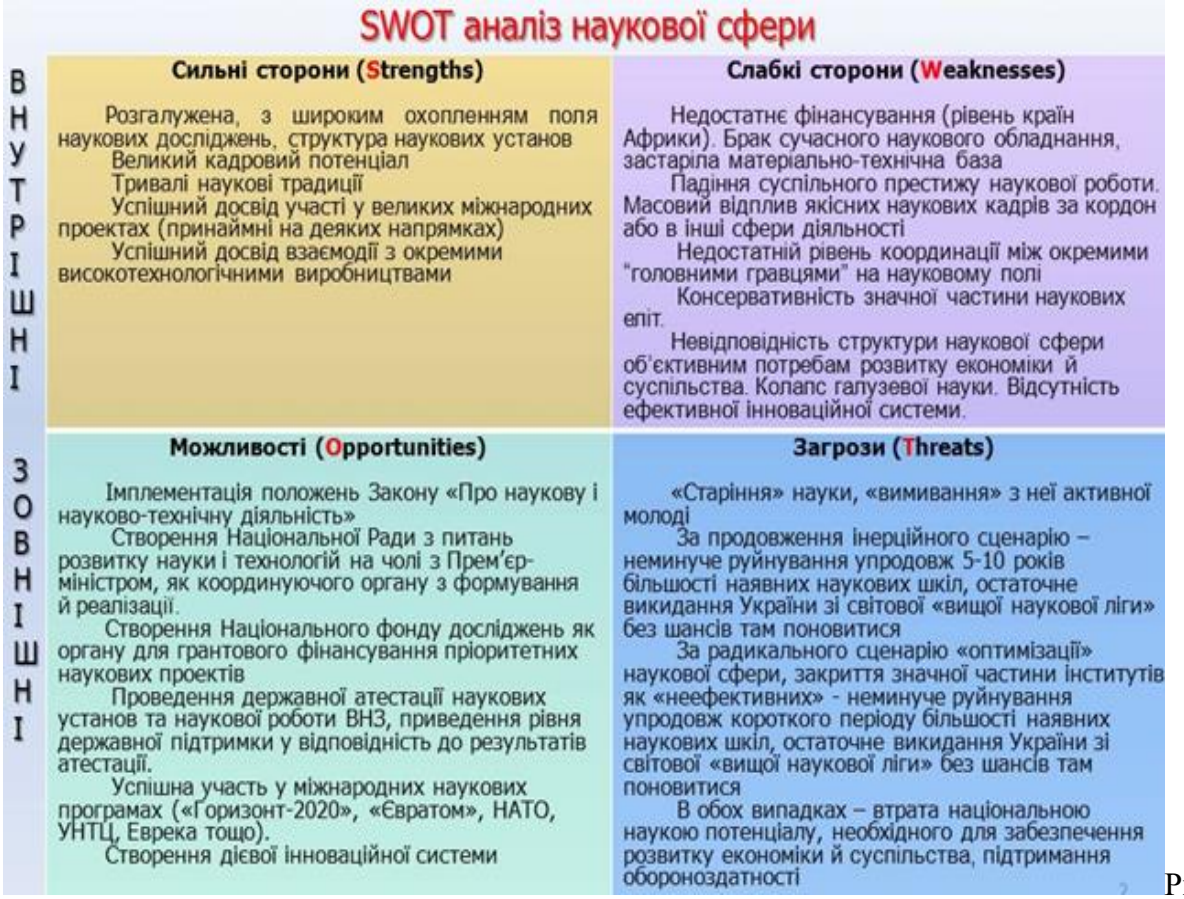


Рис.4.

З того часу ситуація в наукової сфери істотно не покращена і для обдарованої молоді немає мотивації займатися наукою в рідній країні, як би ми її добре не підготували в школі або МАНУ в рамках «STEM-освіти». Тому з кожним роком зростає кількість українських студентів у ЗВО Європи і вона може суттєво зрости після закінчення війни через спад економіки.

Другої глобальною проблемою є неадекватна позиція уряду України щодо статусу ЗВО у сфері підготовки наукових кадрів. Відомо [4], що в провідних ЗВО світу ця підготовка ведеться шляхом інтеграції навчального процесу та фундаментальних наукових досліджень, яка уперше системно була визначена Вільгельмом фон Гумбольдтом що у XIX сторіччі та успішно реалізується в дослідницьких університетах (у 2000 році таких університетів тільки у США було 260, Великобританії – 73, Німеччині – 70, а в Іспанії - 41). За визначенням американського дослідника Дж. Ломбарді, дослідницькі університети генерують найвищий рівень «внутрішньої академічної якості», використовуючи як своєрідне паливо в своїх «двигунах якості» найефективніші ресурси, в першу чергу, людські: професорсько-викладацький, адміністративний, дослідницький персонал, студентів; а також матеріальні, фінансові і інформаційні ресурси. Процес призначення статусу дослідницьких університетів в Україні більш за 30 критеріями діяльності (рис. 5) відбувався за ініціативою НТУУ «КПІ» у 2007—2010 роках [5].

Рис. 5.

Пізніше цій статус було надано 14 ЗВО України, однак, нажаль, за час прем'єрства Арсенія Яценюка статус дослідницьких університетів в державі був тимчасово припинений.

Таким чином, в даний час підготовка фахівців НН ІТС здійснюється за двома головними напрямками трикутника знань (рис. 6): передова освіта та конкурентоспроможна наука. Для впровадження інноваційної діяльності та остаточного введення в навчання принципів «STEM-освіти», необхідно додатково фінансування (рис. 7), що дозволить ІТС і НТУУ «КПІ» в цілому та і іншим ЗВО України технічного напрямку рішить проблему підготовки сучасних фахівців.

Рис. 6

Рис. 7

Література

1. Сакунова Г.В., Мороз І.О. STEM-освіта: зарубіжний досвід та перспективи розвитку в Україні. Наукові записки [Центральноукраїнського державного педагогічного університету імені Володимира Винниченка]. Серія: Педагогічні науки. - 2018, вип. 168, с. 204-208.
2. Подлєсний С.В., Тарасов О.Ф. Актуальність використання STEM-STEAM-STREAM-технологій в сфері інженерно-технічної освіти для сталого розвитку економіки України. Вісник Вінницького політехнічного інституту. – 2019, вип. 2, с. 123-131.
3. Задворнов В. Студентське КБ НН ІТС: робота на перемогу і задля майбутнього. Київський політехнік. – 2023, № 7-8, с. 4.
4. Кузьменко О. М. Місія та завдання дослідницьких університетів та університетів світового класу. ISSN Online: 2312-5829. Освітологічний дискурс, 2014, № 4 (8), с. 179-190.
5. Згуровський М.З., Ільченко М.Ю., Якорнов Є.А. Організація наукових досліджень в галузі телекомунікацій. Підручник. – К.: НТУУ «КПІ» імені Ігоря Сікорського, 2018 – 336 с.

УДК 621.3

НАУКОВА ДІЯЛЬНІСТЬ СТУДЕНТІВ НАВЧАЛЬНО-НАУКОВОГО ІНСТИТУТУ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ КПІ ІМ. ІГОРЯ СІКОРСЬКОГО

Лісовський К.С., Буглак А.В.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: k.lisovskiy@ukr.net, buglachok2003@gmail.com

STUDENTS SCIENTIFIC ACTIVITY OF THE EDUCATIONAL AND RESEARCH INSTITUTE OF TELECOMMUNICATION SYSTEMS IGOR SIKORSKY KYIV POLITECHNICAL UNIVERSITY

This review will present the chronological order of the origin and development of the student "scientific movement," which is actively working on topical research topics at the base of the Educational and Scientific Institute of Telecommunication Systems of the National Technical University of Ukraine "Ihor Sikorskyi Kyiv Polytechnic Institute".

В роботі представлено хронологічний порядок зародження та розвитку студентського «наукового руху», який активно працює над актуальним темами досліджень на базі Навчально-наукового інституту телекомунікаційних систем Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського".

- **Квітень 2021р. –** протоколом №10/2021 Засідання СР НН ІТС створено науковий відділ на базі органу студентського самоврядування НН ІТС КПІ ім. Ігоря Сікорського. Очільник (до травня 2022 року – студентка гр. ТЗ-81 Інна Бутько, з травня 2022р. – студент гр.ТН-21мн Костянтин Лісовський). Відділ сприяє студентському контингенту як у пошуку тем для досліджень, так і у виданнях до публікування (самвидат, журнали, наукові конференції очного/дистанційного/заочно-дистанційного типу тощо).
- **Грудень 2021р.** – презентація модернізованої Wi-Fi мережі НН ІТС, затвердження проєкту до розвитку та впровадження рішенням Вченої Ради НН ІТС від 28.12.2021р. [1].
- **Січень 2022 р.** – наказом №НОН/23/2022 від 20.01.2022 в Навчально-науковому Інституті телекомунікаційних систем зареєстровано гурток «Студентське конструкторське бюро ІТС», який існує й досі [2].
- **Січень 2022 р.** – оновлення локальної радіомережі НН ІТС. Було виконано ряд заходів, а саме: проведення профілактичних робіт, запусків, прокладання додаткової гілки на вихід корпусу №30, тестувальні запуски системи оповіщень (сигнал «УВАГА ВСІМ!» з тривалістю звучання до 20 секунд, попередження про тестування системи–двічі з тривалістю до 10 секунд) [3].
- **Лютий 2022 р.** – профілактичні роботи з оновлення програмного забезпечення діючої бездротової мережі. Оновлення ПЗ було здійснене з метою стабілізації роботи діючої мережі, профілактики “викидів” під час

довготривалого користування та забезпечення стабільної пропускної здатності підключення [4].

- **Лютий 2022 р.** – наукова публікація з теми «Artificial Intelligence in the security system of enterprise» з закордонним авторством [5].
- **Березень 2022 р.** – технічна публікація з теми «Основи роботи антивірусного програмного забезпечення» у співавторстві з абітурієнтами [6].

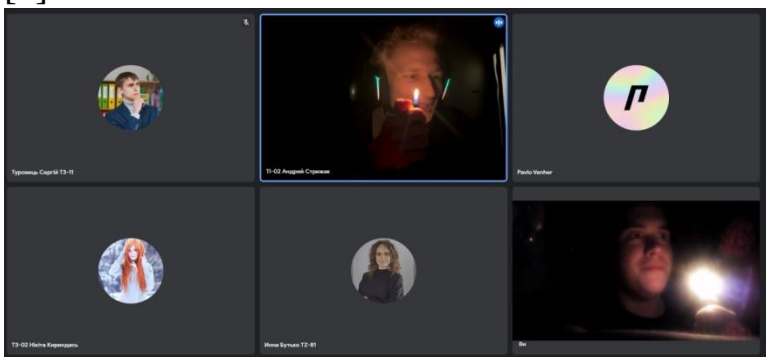


Рис. 1. Засідання робочої групи СКБ під час атак московії.

- **Березень 2022 р.** – створення «кіберфронту» з метою боротьби проти московії у цифровій площині. Активне забивання етеру окупантам на півдні [7].
- **Березень-квітень 2022 р.** – прокладання інтернет-зв'язку у сховищах на території студмістечка КПІ ім. Ігоря Сікорського [8].
- **Квітень 2022 р.** – Наукова публікація-дослідження з актуальної теми «Communication Architecture And Protocols Uav Network» [9].
- **Квітень-травень 2022 р.** – наукова публікація-дослідження з актуальної теми «Огляд та реверс-інженірінг роутеру та Ethernet-адаптеру Dishy Starlink» [10].
- **Травень 2022 р.** – зустріч представників ректорату з адміністрацією та Студентською радою Інституту, обговорення планів масштабування «моделі ІТС» [11].

Рис. 2. Зустріч з адміністрацією КПІ ім. Ігоря Сікорського.

- **Липень 2022 р.** – наукова публікація-дослідження з актуальної теми «Огляд та реверс-інженірінг роутеру STARLINK II покоління» [12].
- **Серпень 2022 р.** – отримання термінального обладнання STARLINK у користування НН ІТС, модернізація обладнання, проведення

виїзних тестувань [13].

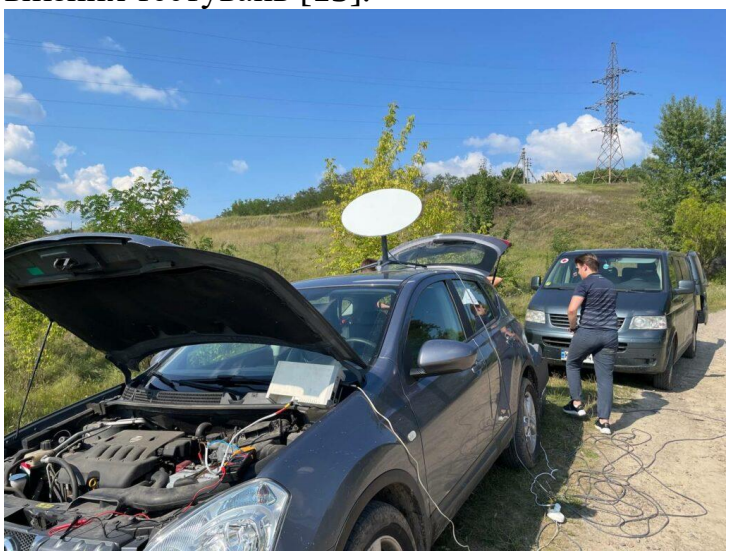


Рис. 3. Виїзне тестування термінального обладнання STARLINK.

- **Вересень 2022 р.** – представлення «пілотної» версії самвидату методичних матеріалів за темою розвідки на основі відкритих даних [14].
- Жовтень 2022 р. – створення робочої групи «Powerbank» на базі СКБ, організація виготовлення powerbank-ів та накопичувачів для Збройних Сил України з перероблених одноразових електронних сигарет.

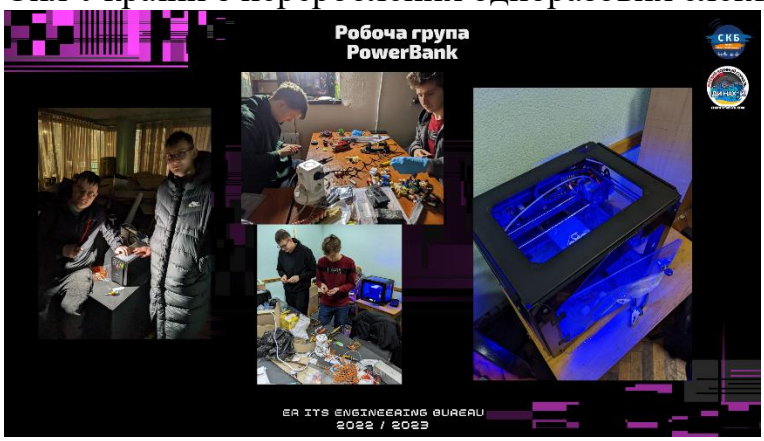


Рис. 4. Звіт СКБ 2022 – слайд про РГ.

- **Листопад 2022 р.** – тестове встановлення термінального обладнання STARLINK у корпусі №30, «стрес-тестування» в умовах графіків погодинних відключень та регулярного навантаження [15].
- **Грудень 2022 р.** – наукові публікації-дослідження з актуальних тем: «THE CONSEQUENCES OF EL-SALVADOR'S ADOPTION OF CRYPTOCURRENCY AS LEGAL TENDER» та «NETWORK LAYER: ITS ARCHITECTURE, SURVEY AND NETWORK SYSTEM» [16], [17].
- **Березень 2023 р.** – наукова публікація за актуальною темою: «POTENTIAL DEVELOPMENT & IMPLEMENTING OF BLOCKCHAIN AND CRYPTOCURRENCIES IN THE EUROPEAN UNION AND THE EUROZONE» [18].

Студентський колектив СКБ НН ІТС КПІ ім. Ігоря Сікорського, слідкує за тенденціями розвитку цифрових технологій при активній допомозі як

студентів, так і наукових керівників створюють технічні описи наукових оглядів та досліджень.

Література

1. Wi-Fi Network Report (перспектива) [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://1drv.ms/w/s!Aj1zZgezaJlDiAlu5SyUIqrPQX9_?e=cSksVL.
2. Наказ №НОН/23/2022 від 20.01.2022 [Електронний ресурс] – Режим доступу до ресурсу: https://drive.google.com/file/d/1_Ph7c3wMy5yWCK_2tAatEzLU6Q_-zQk6/view.
3. RADIO ITS – UPGRADED! [Електронний ресурс] – Режим доступу до ресурсу: https://sr-its.kpi.edu.ua/2022/02/08/radio-its-upgraded/.
4. WIFI ITS – UPGRADED! [Електронний ресурс] – Режим доступу до ресурсу: https://sr-its.kpi.edu.ua/2022/02/12/wifi-its-upgraded/.
5. Lisovskyi K. Artificial Intelligence in the security system of enterprise [Електронний ресурс] / G. Rochenovich, K. S. Lisovskyi. – 2022. – Режим доступу до ресурсу: http://dx.doi.org/10.13140/RG.2.2.23364.50562.
6. Лісовський К. С. ОСНОВИ РОБОТИ АНТИВІРУСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ [Електронний ресурс] / К. С. Лісовський, А. П. Стрижак, П. Венгер. – 2022. – Режим доступу до ресурсу: http://dx.doi.org/10.13140/RG.2.2.36196.45444/1.
7. Перехоплення та «забивання» ефіру членом СКБ [Електронний ресурс] – Режим доступу до ресурсу: https://t.me/scb_its/17.
8. Звернення з питання прокладання інтернет-зв'язку у сховищах та на робочих місцях [Електронний ресурс] – Режим доступу до ресурсу: https://t.me/scb_its/26.
9. Zhivkov A. COMMUNICATION ARCHITECTURE AND PROTOCOLS UAV NETWORK [Електронний ресурс] / A. Zhivkov, N. Kyryndas, K. Lisovskyi – Режим доступу до ресурсу: https://www.researchgate.net/publication/360270164_COMMUNICATION_ARCHITECTURE_AND_PROTOCOLS_UAV_NETWORK
10. Сайченко І. ОГЛЯД ТА РЕВЕРС-ІНЖЕНІРІНГ РОУТЕРУ ТА ETHERNET-АДАПТЕРУ DISHY STARLINK [Електронний ресурс] / І. Сайченко, Р. Камаралі, К. Лісовський. – 2022. – Режим доступу до ресурсу: https://doi.org/10.36074/grail-of-science.29.04.2022.046.
11. Зустріч з адміністрацією КПІ ім. Ігоря Сікорського: ФОТОЗВІТ [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://sr-its.kpi.edu.ua/2022/05/19/admin-meet-19-05-2022/.

12. ОГЛЯД ТА РЕВЕРС-ІНЖЕНІРІНГ РОУТЕРУ STARLINK II ПОКОЛІННЯ [Електронний ресурс] / К.Лісовський, А. Стельник, І. Сайченко, Р. Камаралі // III CISP Conference «SCIENCE OF POST-INDUSTRIAL SOCIETY: GLOBALIZATION AND TRANSFORMATION PROCESSES». – 2022. – Режим доступу до ресурсу: http://dx.doi.org/10.36074/grail-of-science.22.07.2022.040.
13. Студентське Конструкторське Бюро при НН ІТС 7 серпня 2022 року провело виїзне тестування системи супутникового зв’язку STARLINK. [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://sr-its.kpi.edu.ua/2022/09/18/starlink-in-er-its/.
14 Лісовський К. Лекція 1. Вступ до інформаційного простору. Як працювати з пошуковим рушієм на свою користь [Електронний ресурс] / К. Лісовський, А. Буглак, А. Стрижак. – 2022. – Режим доступу до ресурсу: http://dx.doi.org/10.13140/RG.2.2.25316.04483/1
15. 21 вересня 2022 року робоча група СКБ НН ІТС після багаторазових тестів та випробувань пропускної передачі даних встановила систему супутникового зв'язку у корпус! [Електронний ресурс] – Режим доступу до ресурсу: https://t.me/scb_its/104.
16 Lisovskyi K. THE CONSEQUENCES OF EL-SALVADOR'S ADOPTION OF CRYPTOCURRENCY AS LEGAL TENDER [Електронний ресурс] / K. Lisovskyi, N. Kyryndas, G. Rochenovich // V CISP Conference «AN INTEGRATED APPROACH TO SCIENCE MODERNIZATION: METHODS, MODELS AND MULTIDISCIPLINARITY». – 2022. – Режим доступу до ресурсу: http://dx.doi.org/10.36074/grail-of-science.23.12.2022.33.
17 Lisovskyi K. NETWORK LAYER: ITS ARCHITECTURE, SURVEY AND NETWORK SYSTEM [Електронний ресурс] / K. Lisovskyi, A. Stryzhak, M. Herashchenko // V CISP Conference «AN INTEGRATED APPROACH TO SCIENCE MODERNIZATION: METHODS, MODELS AND MULTIDISCIPLINARITY». – 2022. – Режим доступу до ресурсу: http://dx.doi.org/10.36074/grail-of-science.23.12.2022.31.
18 Lisovskyi K. POTENTIAL DEVELOPMENT & IMPLEMENTING OF BLOCKCHAIN AND CRYPTOCURRENCIES IN THE EUROPEAN UNION AND THE EUROZONE [Електронний ресурс] / K. Lisovskyi, G. Rochenovich. – 2023. – Режим доступу до ресурсу: http://dx.doi.org/10.13140/RG.2.2.17659.39204.

УДК 681.327

ЗАСТОСУВАННЯ ГЕНЕТИЧНОГО АЛГОРИТМУ ДЛЯ СИНТЕЗУ ОПТИМАЛЬНОЇ СТРУКТУРИ ТУРБОКОДУ

Лівенців С.П.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail slivencev@gmail.com

APPLICATION OF GENETIC ALGORITHM FOR SYNTHESIS OF OPTIMAL STRUCTURE OF TURBOCODE

The parameters of the target function and the algorithm for searching for the configuration of the turbocode with the help of a genetic algorithm are determined in the work, which will ensure the best efficiency of the communication system under given limitations and conditions.

Нині у сфері телекомунікацій широке застосування знаходять адаптивні системи радіозв'язку. У роботах [1, 2] обговорюється необхідність створення системи зв'язку спеціального призначення (СЗСП), заснованої на використанні розширення спектра та ефективних сигнально-кодових конструкцій, параметри яких змінювалися б залежно від зміни стану каналу зв'язку. Як коригувальні коди можуть бути розглянуті коди БЧХ, Ріда-Соломона, каскадні коди і турбокоди (ТК), а як модуляція – ФМ-М і КАМ-М. Для побудови адаптивної СЗСП виникає необхідність вибору параметрів сигнально-кодових конструкцій (СКК), залежно від зміни стану каналу зв'язку. За винятком ТК, показники завадостійкості СКК описуються аналітичними виразами. Значення ймовірності бітової помилки для ТК виходять, як правило, імітаційним моделюванням [3-6].

Для функціонування адаптивних СЗСП з ТК важливою задачею є вибір оптимальної структури ТК для каналу зв'язку, параметрі якого змінюються в часі.

Задача оптимізації традиційно формулюється у вигляді [7]:

$$\begin{aligned} & f(X) \to \min \\ & g_i(X) \le 0, i = 1,\dots,m \\ & X \in S \end{aligned} \qquad (1)$$

Результат оптимізації має на меті знаходження такого вектору X, який дозволить отримати мінімальне значення функції $f(X)$, що має назву цільової. Область, в якій здійснюватиметься пошук значень вектору X буде обмежена насамперед областю визначення S, до якої належить X, а також множиною обмежень $g(X)$ значення знакового вектору.

Що стосується СЗСП з ТК завдання (1) матиме такі особливості. Цільова функція (ЦФ) $f(X)$ характеризує ефективність передачі (кількісна оцінка ефективності роботи СЗСП). Метою завдання є знаходження такого вектору

конфігурації СЗСП $X = \{x_1, x_2, \dots, x_n\}$ при якому кількість помилок під час передачі інформації була б мінімальною. Компонентами вектору X є параметри, які описують структуру ТК, що застосовується. В рамках роботи розглядається двокомпонентний вектор $X = \{M, P\}$, компоненти якого відповідатимуть кількісті комірок пам'яті, що використовуються при формуванні згорткового ТК (M) та кількість перевірочних біт, що генеруються ТК (P).

Множина обмежень $g(X)$ описує загальну структуру СЗСП, яка повинна залишитися незмінною в процесі пошуку екстремуму: кількість перевірочних біт (P) рекурсивного систематичного згорткового кодера (РССК), кількість елементів комірок пам'яті РССК (M), довжина блоку даних, що передається, використовуваний алгоритм декодування, тип перемежувача, кількість ітерацій декодування; стан каналу зв'язку тощо.

Область визначення S у загальному випадку є компонентно-різнорідною: $S = S^1 \cup S^2 \cup S^3 \cup S^4$, тобто. різні компоненти вектора X можуть належати різним підмножинам, що не перетинаються. Множина S є кінцевою.

Для СЗСП з ТК інформація про функції $f(X)$, $g(X)$, та їх похідних відсутня. Це обумовлене тим, що у досліджуваної системи зв'язку функції $f(X)$, $g(X)$ задаються не у вигляді аналітичного виразу, а як алгоритм.

Розглянуті особливості не дають можливості вирішення завдання оптимізації (1) за допомогою класичних методів, як завдання багатофакторного пошуку екстремуму, тому що функція $f(X)$ не є гладкою по всій області визначення. Однак через те, що область визначення S є кінцевою множиною, завдання може бути вирішене простим перебором всіх можливих значень вектора X. Слід зазначити, що у разі використання достатньо складного РССК, метод перебору буде неприйнятним у зв'язку з тривалими обчислювальними процесами. Тому для вирішення задачі оптимізації бажано застосовувати методи, що забезпечують мінімальний час находження потрібного результату, ніж метод повного перебору. Як такий метод пропонується використовувати генетичний пошук екстремуму ЦФ.

Надалі під конфігурацією ТК мається на увазі поліном, що визначає роботу системи канального кодування/декодування.

Основним питанням при формулюванні задачі оптимізації (1) є вибір ЦФ $f(X)$, яка дозволить кількісно оцінити ефективність роботи СЗСП з ТК, що має конфігурацією X. У цій роботі вибір ЦФ заснований на принципі ітеративного декодування ТК прийнятої бітової послідовності при паралельній конкатенації двох РСЗК [7, 8].

Генетичний алгоритм (ГА) пошуку оптимального значення може бути застосований у ряді випадків, коли традиційні алгоритми пошуку є неефективними або не можуть застосовуватися взагалі [3]. Розглядається ГА, що оперує як дані бітовими послідовностями. Так як поліном РССК визначається бітовою послідовністю, то перетворення полінома в бітовий рядок відбувається таким чином: на перше місце ставиться цифра 1, записуються бітові комбінації, що відповідають за формування перевірочних

символів, потім – бітова комбінація, що формує зворотний зв'язок, і так в залежності від значення P. Наприклад, при $M = 3$ і $P = 2$ для полінома [1,1011/1101,1001/1101] його бітове уявлення буде str=101110011101. Множина подібних рядків утворюють населення. Кожен рядок є одним із можливих розв'язків задачі.

Даний вектор $X = \{M, P\}$. Необхідно визначити str, що задовольняють конфігурації X з найкращим значенням цільової функції. Для кожного рядка популяції обчислюється ЦФ за правилом: $F_i = \frac{\sum_{t=1}^{n} F_t}{n}$ де n – кількість переданих блоків символів.

Традиційні ітеративні алгоритми займаються покращенням єдиного проміжного рішення, яке має наблизитися до точного. Ітеративний ГА на відміну від них працює на користь поліпшення всієї популяції в цілому, а не деякого конкретного значення вектору X. Перевагою ГА пошуку екстремуму у відсутності повного перебору можливих результатів, є його незалежність від складності реалізації СЗСП з ТК.

Параметри ГА при фіксованій кількості ітерацій впливатимуть тільки на швидкість збіжності, але не на швидкість роботи алгоритму. Час роботи ГА буде залежати від кількості ітерацій ГА та кількості рядків у популяції.

У роботи формулюванні та розв’язанні задачі оптимізації пошуку оптимальної конфігурації СЗСП з ТК на підставі генетичного алгоритму

Подальший розвиток роботи пов'язані з використанням структур, отриманих генетичним методом, в автономному адаптивному управлінні роботою СЗСП з ТК.

Література

1. Б. Горлінський, С. Лівенцев, С. Зайцев, В. Барановський. Обґрунтування напрямків модернізації систем радіозв'язку з рухомими об'єктами за рахунок застосування сучасних технологій // IX Міжнародна науково-практична конференція. Безпека інформації у інформаційно-телекомунікаційних системах. Тези доповідей. - 2000. С. 97-98.
2. С. Зайцев, С. Лівенцев, Д. Алексєєв. Застосування турбокодів у спеціальних телекомунікаційних системах // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - Віп.11, 2005 р. - С. 162-167.
3. Зайцев С.В., Лівенцев С.П., Горлінський Б.В. Програма для аналізу характеристик завадостійкості турбокодів // Свідоцтво про реєстрацію авторського права на твір № 15289. Державний департамент інтелектуальної власності України, Київ. - 16.01.2006.
4. Woodard J., Hanzo L. Comparative Study of Turbo Decoding Techniques: An Overview // IEEE Transactions on Vehicular Technology, Vol. 49, Nu. 6, 2000. – Листопад. P. 2208 - 2232.
5. Wang C. На виконанні turbo codes // The aerospace corporation 2350 E. El Segundo Blvd. M1/136. - 1998. P. 3-6.
6. Valenti M. Turbo codes and iterative processing // Virginia Polytechnic Institute and State University Blacksburg. - USA. P. 3-6.
7. Qi J. Turbo код в IS-2000 код дивізії multiple access communications under fading // Wichita State University. - 1999. P. 38-59.
8. Woodard J., Hanzo L. Comparative Study of Turbo Decoding Techniques: An Overview // IEEE Transactions on Vehicular Technology, Vol. 49, Nu. 6, 2000. – Листопад. P. 2208 - 2232.

УДК 621.382

НОВІ КОМПОЗИТНІ ПОСЛІДОВНОСТІ БАРКЕРА В СИСТЕМАХ З ПРЯМИМ РОЗШИРЕННЯМ СПЕКТРУ

Максимов В.В., Носков В.І., Храповицький І.А.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: maksimov46@ukr.net, hrapovitskiy.igor@gmail.com

NEW COMPOSITE BARKER CODES IN SYSTEMS WITH DIRECT SPECTRUM SPREADING

Modeling in the MatLab software package showed the possibility of using new composite Barker codes as code words in direct spread spectrum systems.

На даний час широкосмугові 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. Найкращими кореляційними характеристиками з усіх ШПС володіють послідовності Баркера [1], основний викид АКФ яких дорівнює числу розрядів результуючої послідовності N, а максимальний бічний викид в позитивну область має значення 1. В [2] отримано 4 пари нових композитних послідовностей Баркера, а в [3] ще 28 нових пар, які мають ту ж саму АКФ, що і послідовності з [2]. В [4] досліджена можливість використання нових композитних послідовностей Баркера в якості синхросигналів і показана їх ефективність. В [5, 6] показана ефективність використання нових композитних послідовностей Баркера в якості синхросигналів в порівнянні з послідовностями Голда.

Метою даної роботи є дослідження нових композитних послідовностей Баркера в якості кодових слів в системах з прямим розширенням спектру. В якості кодових слів використовуються нові композитні коди Баркера 21а, 33а, 49, 77а, 121, а в якості сигналів синхронізації композитний код Баркера 121 і код Голда 127-1. Для синтезу кодів Голда 127 в програмі MATLAB R2015B бралися preferred polynomial (1) («переважний поліном») 'z^7+z^3+1' і відповідно preferred polynomial (2) 'z^7+z^3+z^2+1' з довільно обраним вихідним станом регістрів.

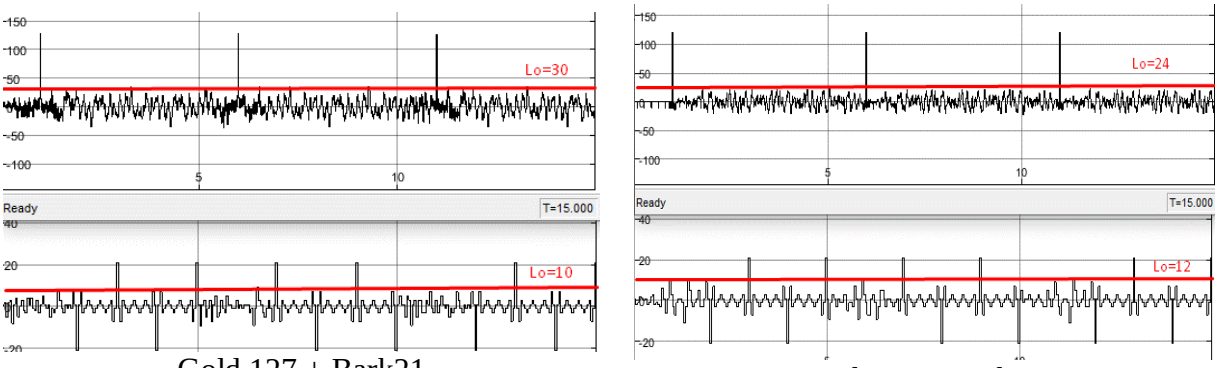
Моделювання режиму прийому ШПС. Схема моделі побудована в програмі MATLAB R2015B і має два блоки формувачів послідовностей синхроімпульсів (СІ) та кодових слів (як прямих (КС) так і інверсних (КСінв)). Генератор імпульсів керує перемикачем і по черзі направляє в канал імпульси синхронізації та кодові слова, утворюючи ШСС, який має наступні цикли: СІ-КСінв-КС-КСінв-КС-СІ-КС-КСінв-КС-КСінв-СІ-КС-… Сформований ШСС поступає на два ідентичні тракти прийому та обробки СІ і прийому та обробки КС та КСінв. Рівень білого Гаусового шуму, що додається до вхідного ШСС встановлюється параметром SNR [dB] блоку AWGN.

В тракті прийому та обробки СІ цифровий узгоджений фільтр ЦУФ-1 виділяє із суміші ШСС і шуму синхроімпульси, схильні до дії перешкод і шуму. На виході ЦУФ-1 утворюються як правильно прийняті СІ, так і імпульси помилкового спрацьовування.

Другий цифровий узгоджений фільтр ЦУФ-2 із ШСС без шумів та перешкод виділяє «еталонні» синхроімпульси. У схемі фіксації помилок із суміші правильних та хибних імпульсів виключаються правильно прийняті, що збігаються з «еталонними», залишаються тільки імпульси хибного спрацьовування, які підраховуються лічильником

помилок СІ. Кожен імпульс помилкового спрацьовування через схему управління рівнем обмеження Lo збільшує поріг обмеження до тих пір, поки шумові та хибні складові не будуть компенсовані. Рівень обмеження фіксується індикатором Lo.

На рис. 1 наведено сигнали на виході трактів прийому та обробки СІ і КС (в якості прикладу взято СІ Gold127 - КС Bark21 і СІ Bark121 - КС Bark21). З рис. 1 видно, що структура циклу не порушена, прямі та інверсні КС чергуються. Також видно, що негативні викиди АКФ кодових інверсних слів стають позитивною завадою для прямих кодових слів.



Gold 127 + Bark21 Bark121 + Bark21

Рис. 1. Сигнали на виході трактів прийому та обробки синхроімпульсів і кодових слів.

Порівняння проводилося за критерієм відсотка втрат пікового значення АКФ при компенсації рівня шумів різних значень SNR (dB) (Signal-to-Noise Ratio). Ефективність різних видів кодових слів оцінювалася за критерієм втрати піку АКФ синхроімпульсу

$$P(\%) = L_0/A, \quad (1)$$

де L_0 - рівень порогу при безпомилковому прийомі, A – амплітуда імпульсу синхронізації, що дорівнює довжині коду.

Ефективність використання кодових слів при різних видах синхроімпульсів оцінювалась параметром

$$\Delta P_{КС}\ (\%) = P_{Bar/Bar}\ (\%) - P_{Bar/Gold}\ (\%), \quad (2)$$

де $P_{Bar/Bar}$ (%) і $P_{Bar/Gold}$ (%) – втрати виділення піку кодових слів при використанні в якості синхроімпульсів композитних кодів Баркера або кодів Голда.

Ефективність використання синхроімпульсів при різних кодових словах оцінювалась параметром

$$\Delta P_{СІ}\ (\%) = P_{СІ\ Bar/Bar}\ (\%) - P_{СІ\ Bar/Gold}\ (\%), \quad (3)$$

де $P_{СІ\ Bar/Bar}$ (%) і $P_{СІ\ Bar/Gold}$ (%) – втрати виділення піку синхроімпульсу композитного коду Баркера або коду Голда при різних кодових словах.

На рис. 2, 3 наведено відповідні графіки втрат піків АКФ КС при СІ Gold 127 і Bark 121.

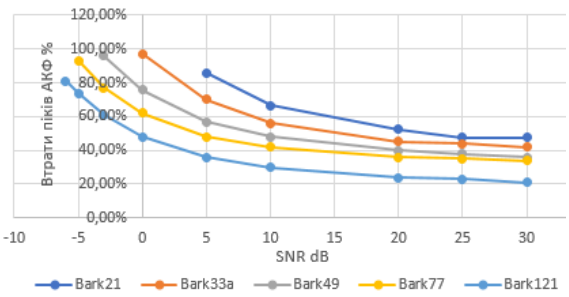


Рис. 2. Втрати піків АКФ КС при СІ Gold 127.

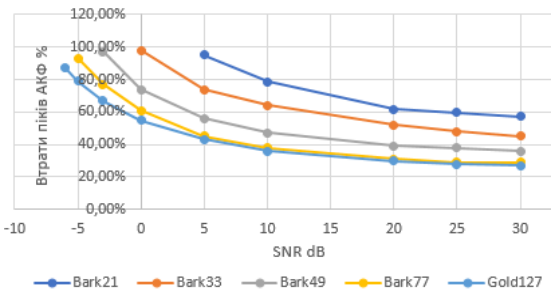


Рис. 3. Втрати піків АКФ КС при СІ Bark 121.

Висновки

1. Аналіз результатів моделювання показує, що нові композитні коди Баркера 21а, 33а, 49, 77а, 121 можуть бути використані в якості кодових слів в широкосмугових системах з прямим розширенням спектру.

2. При використанні композитних кодів Баркера 21а, 33а, 49, 77а, 121 в якості кодових слів їх не слід використовувати з композитними кодами в якості сигналів синхронізації. Так використання композитних кодів в якості кодових слів разом з синхроімпульсом Голд 127 виявилося більш ефективним ніж з синхроімпульсом Баркер 121, а саме:

- коди Баркера 21а в діапазоні зміни SNR (5 ÷ 30) dB більш ефективні на (9,50 ÷ 11,9)%;
- коди Баркера 33а в діапазоні зміни SNR (0 ÷ 30) dB більш ефективні на (1,0 ÷ 8,0)%;
- коди Баркера 49 в діапазоні зміни SNR (-3 ÷ 30) dB більш ефективні на (0,0 ÷ 1,0)%;
- коди Баркера 77а в діапазоні зміни SNR (-5 ÷ 30) dB більш ефективні на (0,0 ÷ -5,0)%;
- коди Баркера 121 в діапазоні зміни SNR (-6 ÷ 30) dB більш ефективні на (5,0 ÷ 7,0)%.

3. Підтверджена ефективність використання композитних кодів Баркера в якості синхроімпульсів в порівнянні з кодами Голда при використанні композитних кодів Баркера в якості кодових слів.

4. Враховуючи, що не всі композитні коди розглядалися в даній роботі, бажано в якості кодових слів додатково розглянути композитні коди 21б, 33б, 49 (Nev2- Nev4), 77б,, 121 (Nev2- Nev4).

Література

1. Barker, R. H. "Group Synchronizing of Binary Digital Sequences". Communication Theory. London: Butterworth. pp. 273–287.
2. Maksymov V., Khrapovitsky I. Research of composite Barker codes // The scientific heritage, № 48 (2020), P.1, p.p. 15-22.
3. Максимов В.В., Храповицький И.А. Нові композитні коди Баркера // The scientific heritage, № 49 (2020), P.1, с.с. 29 – 35;
4. Volodymyr Maksimov, Ihor Khrapovitsky New composite Barker codes in the synchronization system of broadband signals // Information and Telecommunication Sciences, 2020, Number 2, p.p. 24-30.
5. Volodymyr V. Maksymov, Viktor K. Gatturov, Igor A. Khrapovitsky New composite Barker codes, Gold codes and Kasamisequences in broadband signal synchronization systems // Information and Telecommunication Sciences, 2022, Volume 14, Number 1, p.p. 14-21. ISSN 2312-4121.
6. Maksymov V., Noskov V., Khrapovitsky I. New composite codes of Barker and codes Gold in the synchronization system of broadband signals // The scientific heritage, № 94 (2022), P.1, p.p. 110-120.

УДК 623.482

УДОСКОНАЛЕНИЙ МЕТОД ПОБУДОВИ МОДЕЛЕЙ ОЦІНКИ НАДІЙНОСТІ ОБ'ЄКТІВ ЕЛЕКТРОННОГО КОМУНІКАЦІЙНОГО ОБЛАДНАННЯ З КОМБІНОВАНИМ РЕЗЕРВОМ ЧАСУ

Тихонов М.В.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: tichonov@ukr.net

IMPROVED METHOD OF BUILDING MODELS FOR RELIABILITY ASSESSMENT OF ELECTRONIC COMMUNICATION EQUIPMENT OBJECTS WITH COMBINED TIME RESERVE

An improved method has been proposed that allows for the derivation of new analytical formulas to evaluate the key reliability indicators of a system with a combined time reserve, which enables the consideration of various types of failures and malfunctions of technical and software components of electronic communication equipment.

Аналіз, проведений у [1−3], показав, що в об'єктах електронного комунікаційного обладнання (ЕКО) можуть виникати відмови та збої як технічних, так і програмних засобів. У відповідності з ДСТУ [4], під збоєм будемо розуміти самоусуваючу відмову або одноразову відмову, що усувається незначним втручанням оператора. Зокрема, прикладом можуть бути збої програмного забезпечення, одні з яких не потребує перезавантаження ЕКО і мають тривалість, що не перевищує поповнюваний резерв часу $t_д$, при цьому об'єкт не припиняє нормальне функціонування. Інші збої вимагають перезавантаження ЕКО за участі оператора і для відновлення працездатності програмного забезпечення витрачається час, що перевищує допустиме значення $t_д$. У цьому випадку в момент витрачення поповнюваного резерву часу $t_д$ виникає відмова об'єкта і закінчується його функціонування.

У подальшому викладенні збої та відмови будемо називати стійкими відмовами (або просто відмовами), якщо після закінчення поповнюваного резерву часу $t_д$ на відновлення працездатності об'єкта витрачається деякий час.

Особливістю функціонування об'єктів з комбінованим резервом часу є те, що в них передбачені одночасно обмеження на час кожного ремонту об'єкта, а також на сумарний час простою в ремонті (при знецінюючих відмовах – і на повторення всієї або частини попереднього навантаження) до виконання завдання. Хоча в системі об'єкт – час резерв часу є єдиним, зручно при аналізі надійності вважати, що він складається з двох складових: поповнюваної $t_д$ і непоповнюваної $t_р$ [5].

Умови функціонування такої системи ОЧ при досягненні критичного

значення часу відновлення $t_{\text{в}}$ об'єкта, тобто коли воно стає рівним однієї зі складових резерву часу, визначається взаємодією поповнюваної $t_{\text{д}}$ і непоповнюваної $t_{\text{р}}$ складових комбінованого резерву.

Сформулюємо вихідні передумови, обмеження та допущення, при яких будемо вирішувати задачу побудови моделей оцінки надійності об'єктів ЕКО з комбінованим резервом часу. Нехай в об'єкті виникають відмови та збої технічних та програмних засобів i типів $(i \geq 1)$, які можуть призводити до затримки виконання завдання тривалістю $t_{\text{з}} = \text{const}$. Позначимо через $F_i(t) = P\{t_{0i} < t\}$ і $F_{\text{в}i}(t) = P\{t_{\text{в}i} < t\}$ – функції розподілу відповідно напрацювання об'єкта до відмови t_{0i} і часу відновлення $t_{\text{в}i}$, $i \geq 1$. Неважко побачити, що напрацювання об'єкта до будь якої відмови – випадкова величина t_0 з функцією розподілу

$$F_0(t) = P\{t_0 < t\} = 1 - \prod_{i \geq 1} [1 - F_i(t)].$$

Будемо вважати, що напрацювання об'єкта до відмови t_{0i} і час відновлення працездатності $t_{\text{в}i}$ при відмовах i-го типу $(i \geq 1)$ – взаємо незалежні випадкові величини з відомими або заданими функціями розподілу, які мають кінцеві математичні очікування. Відносно поведінки об'єкта після відновлення працездатності приймемо наступні допущення: в момент закінчення ремонту об'єкт з ймовірністю p_i, $0 \leq p_i \leq 1$ продовжує виконувати завдання з урахуванням попереднього напрацювання (при незнецінюючій відмові) або ймовірністю $1 - p_i$ приступає до виконання завдання з самого початку після відновлення об'єкта (при знецінюючих відмовах). Внаслідок затримок, обумовлених виникненням та усуненням відмов, реальний час виконання завдання стає випадковою величиною $T_{\text{вз}}$ з невідомою функцією розподілу.

В об'єкті використовується комбінований резерв часу $(t_{\text{д}}, t_{\text{р}})$ з заданими значеннями поповнюваної $t_{\text{д}}$ і непоповнюваної $t_{\text{р}}$ складових резерву. Взаємодія цих складових $t_{\text{д}}$ і $t_{\text{р}}$ здійснюється у відповідності з наведеною вище моделлю функціонування об'єкта при незнецінюючих і знецінюючих відмовах. Відмова (зрив функціонування) розглядаємої системи об'єкт – час (ОЧ) виникає при виконанні умови $T_{\text{нп}}(t_{\text{з}}) > t_{\text{р}}$ в момент витрачення непоповнюваної складової резерву часу $t_{\text{р}} = 0$ (тут $T_{\text{нп}}(t_{\text{з}})$ – сумарний непродуктивний час).

При теоретичному дослідженні даної системи ОЧ приймемо наступні обмеження та допущення: контроль працездатності об'єкта повний, неперервний та достовірний, що дозволяє виявити відмови об'єкта будь-якого типу в момент їх виникнення; напрацювання між сусідніми відмовами розподілена за тим же законом $F(t)$, що і напрацювання до першої відмови; ремонт повністю відновлює вихідні властивості об'єкта і після його

закінчення негайно відновлюється виконання завдання; кількість відновлень працездатності в оперативному інтервалі часу не обмежується, при цьому час відновлення $t_{\text{в}}$ не залежить від кількості відмов в минулому і розподіляється за законом $F_{\text{в}}(t)$ [6].

Для прийнятих вихідних умов необхідно отримати модель оцінки надійності – розрахункові співвідношення для основних показників надійності розглядаємої системи ОЧ з комбінованим резервом часу.

Алгоритм практичної реалізації даного методу включає в себе сукупність наступних основних взаємопов'язаних операцій: 1. Вибір та обґрунтування варіанту взаємодії поповнюваної $t_{\text{д}}$ і непоповнюваної $t_{\text{р}}$ складових комбінованого резерву часу в процесі функціонування системи ОЧ; 2. На першому етапі – дослідження моделі надійності об'єкта з поповнюваним резервом часу $t_{\text{д}}$ при виконанні часового обмеження $t_{\text{в}} > t_{\text{д}}$ з метою обґрунтування умов, при яких напрацювання до відмови буде близька до експоненціального закону з параметром $\lambda_i^* = \lambda_i q_i$, $i \geq 1$, де $q_i = 1 - F_{\text{в}i}(t_{\text{д}})$; 3. На другому етапі – побудова моделі функціонування об'єкта з непоповнюваним резервом часу $t_{\text{р}}$ з метою перевірки часового обмеження $T_{\text{нп}}(t_{\text{з}}) > t_{\text{р}}$ і отримання наближених розрахункових формул для показників надійності системи ОЧ з комбінованим резервом часу.

Реалізація запропонованого методу дозволяє спростити отримання наукових результатів дослідження – нових розрахункових формул для основних показників надійності системи з комбінованим резервом часу і дає можливість сумісно враховувати різні типи відмов та збоїв технічних і програмних засобів ЕКО та параметри використовуваної надлишковості.

Література

1. Ahmad W. Formal reliability and failure analysis of ethernet based communication networks in a smart grid substation /W. Ahmad, O. Hasan, S. Tahar // Formal aspects of computing 32, January (2020): 71–111. DOI: 10.1007/s00165-019-00503-1.
2. Jin Y. Estimating Component Reliability Based on Failure Time Data from a System of Unknown Design. Statistica Sinica / Y. Jin, P. Hall, J. Jiang, F. Samaniego// Statistica Sinica. − 2017. − № 27. – P.479 – 499. DOI:http://dx.doi.org/10.5705/ss.202015.0209.
3. Zhu P. Reliability and Criticality Analysis of Communication Networks by Stochastic Computation/ P. Zhu, J. Han, Y. Guo, F. Lombardi // IEEE Network. – 2016. − №30, Iss. 6. − P. 70 – 76. DOI: https: //doi.org10.1109/mnet.2016.1500221nm.
4. ДСТУ 2860-94. Надійність техніки. Терміни та визначення. Держстандарт України [Електронний ресурс]. − http://www.ksv.biz.ua/publ/dstu/dstu_2860_94/3-1-0-1102.
5. Mogilevich D. Improved Estimates for the Reliability Indicators of Information and Communication Network Objects with Limited Source Information. / D. Mogilevich, I. Kononova // Springer Nature Switzerland (2019): 101-117. DOI: 10.1007/978-3-030-16770-7_5.
6. Mogylevych D. Analytical Model with Interruption of Service of Short-term Objects with Temporary Reservation/ D. Mogylevych, B. Kredentser, I. Kononova, V. Mohylevych // IT&I-2020 Information Technology and Interactions, December 02–03, 2020, CEUR-WS.org, online http://ceur-ws.org/Vol-2845/.

УДК 621.382

ДОСЛІДЖЕННЯ ВПЛИВУ ФАКТОРУ САМОПОДІБНОСТІ НА ФУНКЦІОНУВАННЯ СМО

Уривський Л. О., Сколець А. В.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, м. Київ, Україна
E-mail: leonid_uic@ukr.net, kriklivanastya@gmail.com

STUDY OF THE INFLUENCE OF THE SELF-SIMILARITY FACTOR ON THE FUNCTIONING OF THE QS.

One of the characteristics of modern telecommunications networks is the self-similarity property, due to which load ripples occur in the network at different random time intervals, which can lead to long delays and packet losses. The paper compares the traditional QS model with the Poisson distribution and QS with the Weibull distribution, which describes the self-similarity property. A quantitative assessment of the difference in the characteristics of the models is given, and the importance of taking into account the self-similarity factor when calculating QS quality indicators is shown.

Останнє десятиліття ознаменувалося істотним досягненням у сфері теорії телетрафіку [1, 2] – відкриттям самоподібних властивостей процесів, що протікають у сучасних мережах. Вперше про самоподібний телетрафік заговорили з моменту його відкриття в 1993 році групою вчених W.Leland, M.Taqqu, W.Willinger і D.Wilson [3], які досліджували Ethernet-трафік у мережі корпорації Bellcore і виявили, що вхідні потоки від джерел дискретної інформації є корельованими (на відміну від властивостей речового трафіку із незалежними вхідними потоками), тобто мають властивість самоподібності.

Г. Херст [4] був першим, хто використав специфічний показник для виміру в явищах ступені самоподібності, яка зараз визнається присутньою в багатьох процесах, що пояснюють природні та штучні події.

Отже, кількісною мірою ступеня самоподібності трафіку є показник Херста H, який може набувати значень в інтервалі від 0,5 (фактична відсутність прояву самоподібності) до 1 (максимальна ступінь самоподібності, яка на практиці не зустрічається). Що ближче цей параметр до одиниці, то яскравіше проявляються самоподібні властивості [5].

Для опису СМО використано розподіл Вейбулла [6], як найбільш адекватний в моделях СМО із самоподібністю. Оригінальність дослідженню придає акцент на характеристики, що забезпечують необхідну якість обслуговування.

Для доведення важливості врахування фактору самоподібності проведено графічне порівняння показників якості обслуговування при розподілі Пуассона і розподілі Вейбулла, використовуючи програмне

забезпечення “Matlab” для розрахунку значення σ (сігми) для параметру Херста рівним 0.6, 0.7 та 0.8, та ПЗ “Excel” для розрахунку формул для отриманих значень та побудови самих графіків.

Розглядаючи розподіл Пуассона і розподіл Вейбулла для дослідження показника $W_{оч}$ (Середній час очікування заявки в черзі) використано формули [7, 8]:

Пуассон (M/M/1/∞)

$$W_{оч} = \frac{\rho}{\mu \cdot (1-\rho)} \quad (1)$$

Вейбулл (M/M/1/∞)

$$W_{оч} = \frac{\sigma}{\mu \cdot (1-\sigma)} \quad (2)$$

Для наглядного порівняння розраховано залежність показника $W_{оч}$ у відсутності самоподібності в трафіку при розподілі Пуассона (H = 0.5) та при урахуванні самоподібності (H > 0.5). В Таблиці 1 досліджено даний показник при інтенсивності обслуговування μ= 1,25.

Табл. 1. Залежність показника $W_{оч}$ при розподілах Пуассона (H = 0.5) та Вейбулла (H > 0.5).

ρ	0,5				0,6				0,7				0,8			
H	0,5	0,6	0,7	0,8	0,5	0,6	0,7	0,8	0,5	0,6	0,7	0,8	0,5	0,6	0,7	0,8
Woч	0,75	1,1	1,9	4,5	1,2	1,7	2,5	6,7	1,9	2,5	4,1	10,7	3,2	4,4	7	19,2
Розбіжність	**1**	**1,47**	**2,53**	**6**	**1**	**1,42**	**2,08**	**5,58**	**1**	**1,32**	**2,16**	**5,63**	**1**	**1,38**	**2,19**	**6**

Тоді отримуємо такі графічні залежності при заданих значеннях параметру Херста:

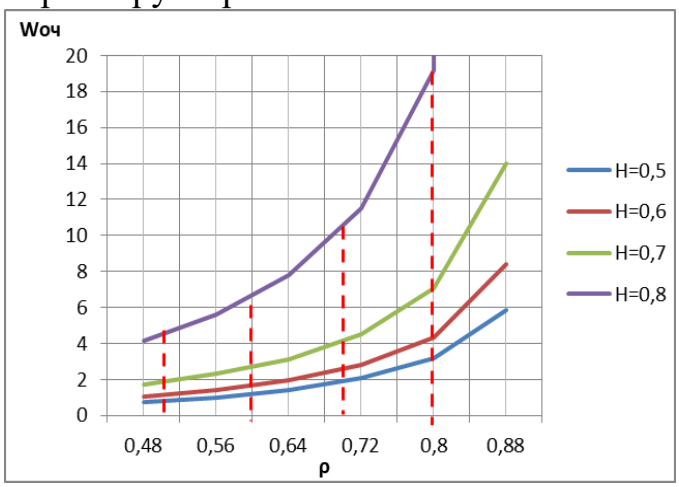


Рис. 1. Середній час очікування при різних значеннях параметру Херста.

Графік залежностей зображений в діапазоні інтенсивності обслуговування від 0.48 до 0.88 і середнього часу очікування від 0 до 20.

Характер наданої залежності такий, що розбіжність в показниках зростає по мірі зростання інтенсивності вхідного потоку та, одночасно, фактору самоподібності і досягає значень близько 6 при суттєвій мірі самоподібності (H = 0,8).

При інтенсивності обслуговування μ = 2 таблиця з залежностями має вигляд:

Табл. 2. Залежність показника $W_{оч}$ при розподілах Пуассона та Вейбулла (μ = 2).

P	0,3				0,4				0,5				0,6			
H	0,5	0,6	0,7	0,8	0,5	0,6	0,7	0,8	0,5	0,6	0,7	0,8	0,5	0,6	0,7	0,8
Woч	0,2	0,3	0,5	1,4	0,3	0,5	0,8	2	0,5	0,7	1,2	2,8	0,8	1	1,7	4,1
Розбіжність	**1**	**1,5**	**2,5**	**7**	**1**	**1,67**	**2,67**	**6,67**	**1**	**1,4**	**2,4**	**5,6**	**1**	**1,25**	**2,13**	**5,13**

Для даного набору значень отримуємо таку графічну залежність:

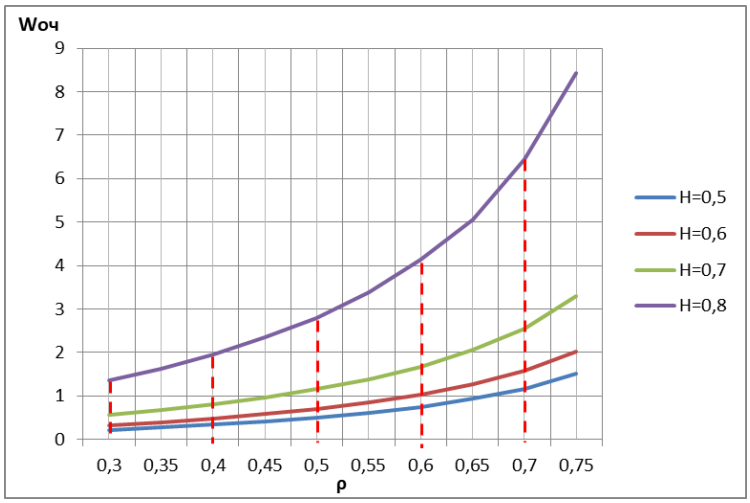


Рис. 2. Середній час очікування при різних значеннях параметру Херста.

Розбіжність досягає значень від 5 до 7 при суттєвій мірі самоподібності (H = 0,8).

Для порівняння дослідимо залежності при μ = 2.25.

Табл. 3. Залежність показника $W_{оч}$ при розподілах Пуассона та Вейбулла (μ = 2,25).

ρ	0,3				0,4				0,5				0,6			
H	0,5	0,6	0,7	0,8	0,5	0,6	0,7	0,8	0,5	0,6	0,7	0,8	0,5	0,6	0,7	0,8
Wоч	0,2	0,3	0,5	1,1	0,3	0,4	0,6	1,7	0,5	0,7	1	2,5	0,7	0,9	1,5	3,7
Розбіжність	1	1,5	2,5	5,5	1	1,33	2	5,67	1	1,4	2	5	1	1,29	2,14	5,29

Далі отримуємо графічну залежність:

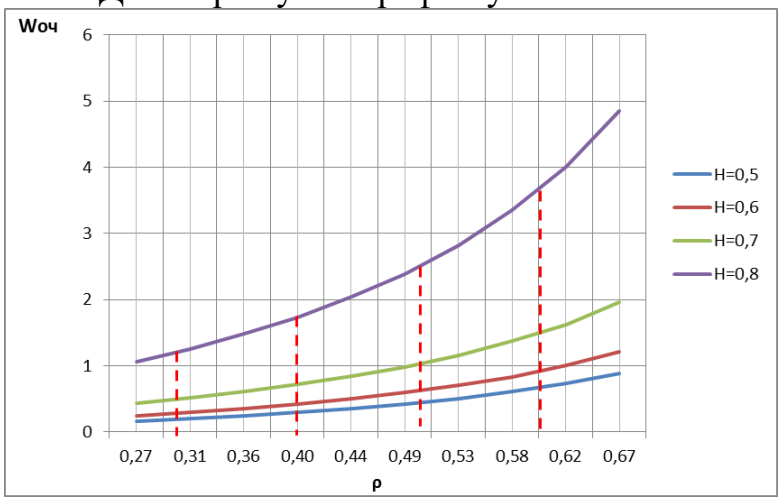


Рис. 3. Середній час очікування при різних значеннях параметру Херста

Аналізуючи отримані графіки, можна зробити загальний висновок, що, якщо не враховувати характеристику ступені самоподібності трафіку, тобто параметр Херста H, то неможливо адекватно представити характеристики для задоволення якості обслуговування в хмарному середовищі.

Висновки. В статті досліджено, як зміни інтенсивності обслуговування впливають на якісні показники системи масового обслуговування, коли має місце самоподібний трафік. Самоподібність описується параметром Херста в інтервалі від 0.5 до 1.

Методики знаходження значень параметрів якості обслуговування в СМО досліджено за допомогою формул Літтла, який є одним із основоположників теорії масового обслуговування.

На графіках зображена залежність середнього часу від інтенсивності навантаження при певних значеннях інтенсивності обслуговування і параметру Херста. Можна помітити, що збільшення середнього часу очікування обумовлено як збільшенням інтенсивності навантаження, так і збільшенням ступені самоподібності. При $\mu = 2$ і зміні інтенсивності обслуговування в діапазоні від 0,3 до 0,75 отримані результати демонструють зміну значення середнього часу змінюється від 0,2 до 1,5 при найпростішому потоці (H = 0,5) та від 1,4 до 8,4 при самоподібності з параметром Херста H = 0,8. При $\rho = 0,3$, розбіжність в часі очікування досягає 7, а при $\rho = 0,7$ розбіжність значень досягає 5,4.

Отже, в разі ігнорування фактору самоподібності система обслуговування не буде відповідати очікуваним параметрам, що може призвести до суттєвої помилки у визначенні кількісних значень характеристик СМО, необхідних для забезпечення потрібної якості обслуговування користувачів.

Література

1. Kleinrock L., Queueing Systems, Vol. I, II, John Wiley & Sons, 1975.
2. Little, J.D.C. (1961): A Proof for the Queueing Formula L = λW. Operations Research, Vol. 9 (1961), pp. 383–387.
3. Leland W.E., Taqqu M.S., Willinger W., and Wilson D.V. On the self-similarnature of ethernet traffic // IEEE/ACM Transactions of Networking, 2(1), 1994. — P.1-15.
4. Hurst, H.E. (1951). "Long-term storage capacity of reservoirs". Transactions of the American Society of Civil Engineers. v.116, p.770.
5. Струбицький Р. П. «Самоподібна модель завантаженості хмарових сховищ даних». Вісник Національного університету «Львівська політехніка». – 2015. – № 14. – С. 147–156.
6. Weibull, W. A statistical distribution function of wide applicability. J. Appl. Mech. 1951, 18, 293–297.
7. Уривський Л.О., Криклива А. В..(2022) ДОСЛІДЖЕННЯ ДИНАМІКИ ПОКАЗНИКІВ ОБСЛУГОВУВАННЯ В СМО ІЗ САМОПОДІБНИМ ТРАФІКОМ./ XVI Міжнародна науково-технічна конференція студентів та аспірантів «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем» ПРІТС-2022: Збірник матеріалів конференції К.: НТУУ «КПІ». – 2022. – с.53-58.
8. Uryvsky L., Kryklyva A. Analysis of Differences in the Characteristics of Queuing Systems with the Dynamics of Input Streams Self-Similarity / Information & Telecommunication Sciences. – V. 13, № 1, 2022. – p.p. 22-26.

УДК 621.391

ОЦІНКА ПОТЕНЦІЙНИХ МОЖЛИВОСТЕЙ РАДІОКАНАЛІВ МОБІЛЬНИХ МЕРЕЖ 5G

Носков В.І.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: nvi2010@ukr.net

ESTIMATION OF POTENTIAL POSSIBILITIES FOR 5G MOBILE NETWORKS RADIOCHANNELS

The report is devoted to results of studies such key indicators (KPI) of the 5G mobile radio access network (IMT-2020), as the bandwidth of radio channels, delay and spectral efficiency. The 5G radio network uses the modern technologies such as OFDM with subcarrier modulation from BPSK to QAM256, antenna systems based on the principle of massive MIMO and with the function of beamforming in the direction of user concentration, interference-resistant coding and other techniques used in modern digital radio systems. The purpose of the research was trying to find the potential possibilities of the 5G radio channel concerning bandwidth, delay and spectral efficiency.

Доповідь присвячена результатам досліджень таких ключових показників (KPI) мережі радіодоступу мобільного зв'язку 5G (IMT-2020), як перепускна здатність радіоканалів, затримка та спектральна ефективність. В радіомережі 5G використовуються такі новітні технології як OFDM з модуляцію піднесучих від BPSK до QAM256, антенні системи за принципом масивних MIMO та з функцією формування променів у напрямку концентрації користувачів, завадостійке кодування та інші техніки, які використовуються в сучасних цифрових радіосистемах. Метою досліджень було намагання знайти потенційні можливості радіоканалів мережі 5G відносно перепускної здатності, затримки та спектральної ефективності.

Створення радіоканалів в мережі мобільного зв'язку 5G відбувається за рахунок використання сучасних технологій таких як OFDM та massive MIMO. Також оптимізовані фрейми та вдосконалений розподіл частотно-часових ресурсів як на Downlink, так і на Uplink. Все це відображено у специфікації радіоінтерфейсу 5G-NR (5G - New Radio). Серед ключових показників якості радіоканалів значущими є пікова швидкість передачі, затримка та спектральна ефективність. Тому дослідження проводились саме для цих показників.

Як рекомендовано в [1], оціночний розрахунок пікової швидкості в напрямку Downlink може проводитись за формулою:

$$R_{\text{пік}} = 10^{-6} \sum_{j=1}^{j} (\vartheta_{Layers}^{(f)} \times Q_m^{(f)} \times f^{(f)} \times R_{m.LDPC} \times \frac{N_{PRB}^{BW(f),\mu} \times 12}{T_S^{\mu}} \times (1 - OH^{(j)})), \quad (1)$$

де: J – кількість агрегованих компонентних несучих у смузі частот або комбінації смуг (максимум 16); $R_{m.LDPC}$ = 948/1024 - максимальна відносна швидкість завадостійкого кодування LDPC; $\vartheta_{Layers}^{(f)}$ – максимальна кількість

потоків від передавача базової станції gNB у напрямку терміналів користувачів; $Q_m^{(f)}$ – кратність модуляції QAM; $f^{(f)}$ = 1; 0,8; 0,75; 0,4 – масштабуючий коефіцієнт; μ = 0; 1; 2; 3 – номер смуги частот однієї піднесучої – 15, 30, 60, 120 кГц, відповідно; $T_S^{\mu} = \frac{10^{-3}}{14 \times 2^{\mu}}$ - середня тривалість символу OFDM у субкадрі відповідно до номеру смуги частот однієї піднесучої; $N_{PRB}^{BW(f),\mu}$ – максимальна кількість ресурсних блоків у смузі частот, що використовується; OH – частка часу, яка витрачається на службові дані у напрямку Downlink. OH = 0,14 для діапазону FR1 (450…6000 МГц) та 0,18 – для діапазону FR2 (24250… 52600 МГц).

Кількість ресурсних блоків, що можуть бути використані в смузі частот, залежить від смуги частот однієї піднесучої (SCS – Subcarrier Channel Space) та загальної смуги частот [2].

За формулою (1) виконані розрахунки максимальної пікової швидкості для максимальної кратності модуляції QAM256, яка дорівнює 8, MIMO 8x8, різних смуг піднесучої та загальних смуг частот, що використовуються в мережі. Результати розрахунків наведені у вигляді графіків на рис. 1.

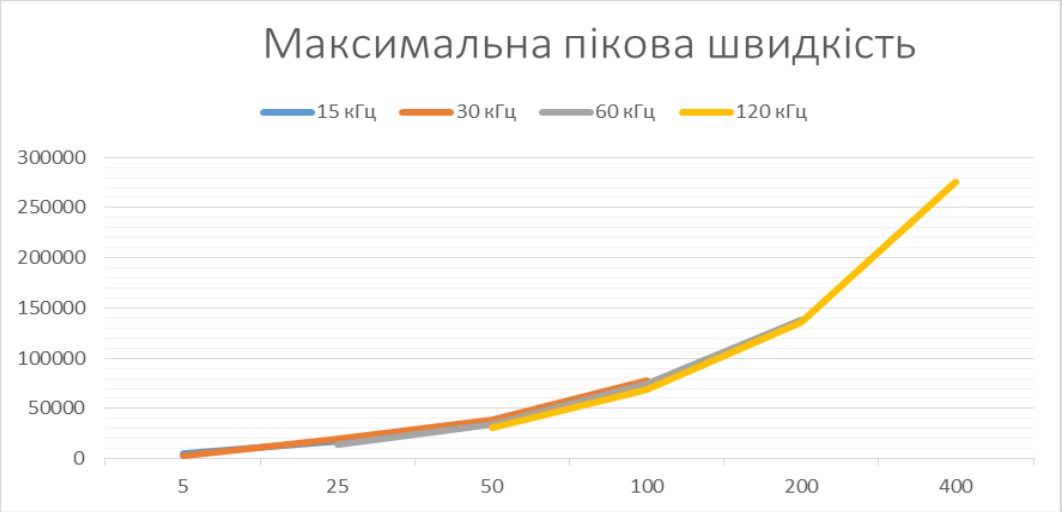


Рис. 1. Залежність максимальної пікової швидкості (Мбіт/с) для QAM256 від смуги піднесучої та загальної смуги частот.

Максимальна пікова швидкість передачі становить 275 Гбіт/с і досягається при використанні смуги піднесучої 120 кГц, кількості піднесучих 16 і загальній смузі частот у 400 МГц.

Затримка в передачі для площини користувача (UPL) визначається як затримка при передачі даних між gNB і UE (User Equipment), тобто час від моменту передачі IP-пакету, до моменту коли приймач успішно приймає IP-пакет і доставляє пакет на верхній рівень. Для розрахунку затримки використовувалась методика та модель, що наведена в [3]. Модель для розрахунку наведена рис. 2.

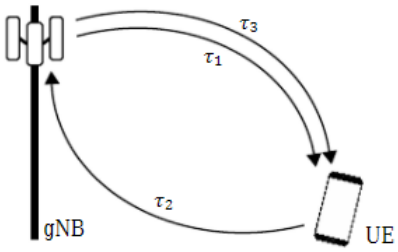


Рис. 2. Модель для розрахунку затримки.

Затримка складається з безпосередньо затримки передачі (τ1), запиту HARQ (Hybrid Automatic Repeat Request) (τ2) і повторної передачі (τ3) між обома об'єктами. Час затримки відповідно до наведеної моделі можна визначити за формулою:

$$\tau = \tau_1 + p(\tau_2 + \tau_3),$$

де: p - вірогідність повторної передачі; $\tau_1 = t_{gNB,tx} + t_{FA1} + t_{TTI} + t_{UE,rx}$; $t_{gNB,tx} = \frac{\max(N_2(2048+144)*k*2^{(-\mu)}*T_c)}{2}$ - тривалість обробки пакетів в базовій станції; t_{FA1} - час, необхідний для вирівнювання кадру або час очікування наступного доступного DL (Down Link) слоту; t_{TTI} - час передачі даних; $t_{UE,rx}$ - час обробки в UE.

Мінімальна затримка відповідає p =0 і залежить від смуги частот піднесучої. Розрахунки дають наступні результати для різних SCS: 15кГц – 1,8мс; 30 кГц – 1,91мс; 60кГц – 2,08мс.

Пікова спектральна ефективність може бути розрахованою за наступною формулою:

$$\eta_p = \frac{\gamma_p}{\alpha * BW},$$

де: γ_p – пікова швидкість передачі; α – коефіцієнт використання частотних ресурсів; BW – смуга частот, що використовується в мережі.

Результати розрахунків η_p у біт/с/Гц наведені в таблиці:

		Смуга DL- 25 МГц		Смуга DL- 50 МГц	
Діапазон FR1	Ширина спектру піднесучої	η_p SISO (без MIMO)	η_p MIMO	η_p SISO (без MIMO)	η_p MIMO
	15	5,7	45,5	5,8	46,2
	30	5,6	44,5	5,7	45,5
	60	5,3	42,5	5,6	44,5

Література

1. 3GPP TS 38.306 version 15.15.0 Release 15. 5G; NR; User Equipment (UE) radio access capabilities – 2021.
2. 3GPP TS 38.101-1 version 15.5.0 Release 15. 5G; NR; User Equipment (UE) radio transmission and reception – 2019.
3. 3GPP TR 37.910 version 16.1.0 Release 16. 5G; Study on self-evaluation towards IMT-2020 submission – 2020.

УДК 621.39

СТРУКТУРИ ОПТИЧНИХ СЕКЦІЙ ЛІНІЙНИХ ТРАКТІВ ВОСП СУ ІЗ ГРАНИЧНО МІНІМАЛЬНИМ *OSNR*

Бердников О.М.
Інститут спеціального зв'язку та захисту інформації КПІ ім. Ігоря Сікорського, Україна
E-mail: 2507bom@gmail.com

OPTICAL SECTIONS LINEAR PATHS STRUCTURES OF FOTS WDM WITH EXTREMELY MINIMAL OSNR

Improvement of the optical signal / noise ratio (OSNR) coefficient in each optical path formed by the VOSP SU is possible due to the reduction of amplifiers of intermediate points of the linear path. The results of long optical sections of OASs transformation that meet the requirements of ITU-T Rec. G.692 on the working attenuation of amplification sections and the sections length on which it is possible to obtain the minimum limit OSNR are provided.

Останні десятиліття характеризуються явно вираженим процесом інтеграції інформаційних систем та телекомунікаційних технологій, що у теперішньому часі пов'язаний з цифровізацією суспільства, зокрема, в Україні, яка стрімко підвищує свої позиції, в тому числі на *digital*-ландшафті Європи. Реалізація цього процесу вимагає неухильного збільшення пропускної спроможності Національної телекомунікаційної мережі України (НТМУ), підвищення її гнучкості, забезпечення ефективної маршрутизації при передачі текстової та мовної інформації, рухомих і нерухомих візуалів, інших мультимедійних послуг. Серед основних компонентів НТМУ, що безпосередньо відповідають за пропускну спроможність мережі, є оптичний сегмент транспортної платформи, який сформовано телекомунікаційними транспортними системами (ТТС). Інтегральною оцінкою таких систем як раз є пропускна спроможність, що визначається швидкістю та дальністю передачі лінійного сигналу. В якості ТТС на телекомунікаційних транспортних мережах і мережах доступу ще з кінця минулого століття успішно використовуються волоконно-оптичні системи передавання (ВОСП).

За цей період вони зазнали помітної трансформації в бік збільшення швидкостей передачі сигналів в оптичних лінійних трактах (ОЛТ) ВОСП. Якщо при використанні каналоутворюючої апаратури (КУА) плезіохронної цифрової ієрархії вона становила десятки і сотні мегабіт в секунду, при переході до КУА синхронної цифрової ієрархії – 10 і 40 Гбіт / с. В теперішній час швидкості передачі сигналів в ОЛТ, що використовують технологію спектрального ущільнення (СУ) (*WDM – Wavelength Division Multiplexing / WDM*) тільки для *C*-діапазону довжини хвиль (найбільш використовуваний в Україні) складають терабіти в секунду [1, 2]. Оптичний сегмент транспортної платформи НТМУ сформовано ВОСП, що використовують технологію спектрального ущільнення (ВОСП СУ). Такі ВОСП СУ мають класичну структуру будови ТТС, яка складається з обладнання кінцевих (КП) та

проміжних пунктів (ПП), що з'єднані одномодовими оптичними волокнами (ООВ) оптичних кабелів (ОК) рис. 1.

Обладнання кінцевих пунктів (КП) формується з оптичних, фотонних лінійних терміналів (*PLTs – Photon Line Terminals*), а проміжних пунктів (ПП) з оптичних лінійних підсилювачів (*OLAs – Optical Line Amplifiers*), які складають оптичний, фотонний лінійний тракт *(PLP – Photon Line Path)*.

Основними пристроями термінала *PLT* є оптичні мультиплексор і демультиплексор (*Optical Multiplexer* і *Demultiplexer* (*OMX* і *ODMX*)) та підсилювачі – оптичний бустер (*OB – Optical Booster*) на передачі й оптичний передпідсилювач (*OP – Optical PreAmplifier)* на прийомі [1].

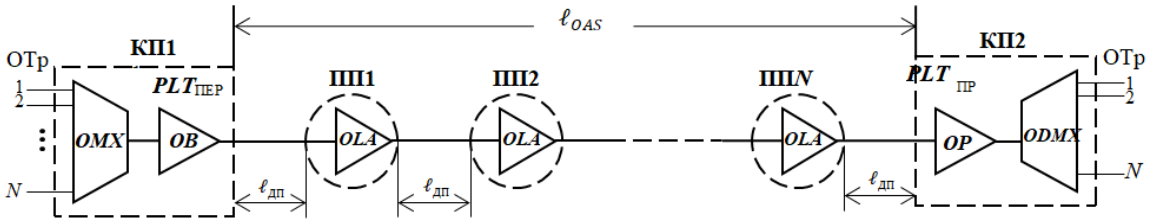


Рис. 1.

Ключова особливість ВОП в тому, що вони є широкосмуговими (ШСМ) або надширокосмуговими підсилювачами. ШСМ ВОП працюють, наприклад, у *C*- або *L*- діапазоні довжин хвиль–λ та посилюють мультиплексний оптичний сигнал $\lambda_{1+2+3+\ldots+N}$ у діапазоні 4…5 ТГц з нерівномірністю АХХ не більше ± 1 дБ. Однак, ВОП "шумлять" тобто, здійснюючи посилення мультиплексного сигналу $\lambda_{1+2+3+\ldots+N}$ у лінійному тракті, вони вносять додатковий шум, який враховується коефіцієнтом відношення оптичний сигнал / шум (*OSNR – Optical Signal to Noise Ratio*) у кожному оптичному тракті (ОТр), що утворений ВОСП СУ. У ВОСП різних технологій СУ (*DWDM, HDWDM, NWDM*) тестування з коефіцієнта помилок по бітах (*BER – Bit Error Rate*) проводиться для кожного утвореного ОТр. При тестуванні ОТр по *BER* використовують однозначну функціональну залежність $BER=\varphi$ (С/Ш), де коефіцієнт помилок є функцією *BER* тобто відношення *OSNR* потужності сигналу ($P_С$) до потужності шуму ($P_Ш$). Для двійкових цифрових сигналів такою функцією є функція Крампа, для неї існують відповідні таблиці. Тоді, вимір *BER* еквівалентний вимірюванню *OSNR*. Тому, щоб підтримувати задане *OSNR* на виході ОТр, що утворюється, число *OLAs* в лінійному тракті повинно бути обмежене.

Найближчі пункти *PLP* з'єднані стандартизованими ділянками посилення (ДП) з оптичних волокон різних типів з довжинами $\ell_{ДП}$, км рис. 1. Такі ДП через ООВ ОК з'єднують вказані елементи лінійних трактів. У ВОСП СУ для побудови їх *PLPs* застосовуються всі три групи типів ООВ: *SF*, *DSF* и *NZDSF*.

Сукупність декількох ДП складають оптичну секцію посилення **(***OAS – Optical Amplifier Section*) – це частина *PLP* між двома будь-якими сусідніми пунктами доступу або елементами мережі, в яких *PLP* розділяється на ОТр. Секції *OASs* можуть бути короткими, середніми і довгими. Короткі *OASs* (50…80 км), як правило, не містять ВОП. Середні *OASs* (120…150 км) зазвичай містять оптичні бустери-*OB* і передпідсилювачі-*OP*. Довгі секції

OASs (600…800 км), крім *OB* та *OP*, містять кілька підсилювачів *OLAs*.

Документами *ITU-T* Рек. *G*.692 в структурі довгих секцій *OASs* рекомендовано використовувати три варіанти довгих ділянок ДП. *L* (*Long*) – довгі ДП це ділянки ООВ до 80 км з затуханням (a_P^L) до 22 дБ, тоді коефіцієнт затухання ООВ буде не більше α_L = (22 дБ)**:**(80 км) = 0,275 дБ/км. *VL* (*Very Long*) – дуже довгі ДП це ділянки ООВ до 120 км з затуханням (a_P^{VL}) до 33 дБ, тоді коефіцієнт затуханням ООВ буде не більше α_{VL} = (33 дБ):(120 км) = 0,275 дБ/км. *UL* (*Ultra Long*) – наддовгі ДП це ділянки ООВ протяжністю до 160 км з затуханням (a_P^{UL}) до 44 дБ, тоді коефіцієнт затуханням ООВ буде не більше α_{UL} = (44 дБ)**:**(160 км) = 0,275 дБ/км. Як видно, всі рекомендовані ДП секції *OAS* типу *L*, *VL*, *UL* з різними довжинами мають однакове значення коефіцієнта затухання ООВ (α). На практиці при будівництві *PLPs* це не виконується.

Згідно Рек. *ITU-T G*.692 кожний тип ДП визначається робочим затуханням ($a_P^{ДП}$), довжиною *OAS* (ℓ_{OAS}) та кількістю ДП ($n_{ДП}$), що надано в табл. 1 стрічками, які виділені сірим кольором.

Загальну структуру *OASs PLPs* ВОСП СУ пояснює рис. 1, на якому надані *OLAs* ПП, що вносять максимальну долю шумів *PLPs* в кожний ОТр. Зі зменшенням шумів покращується коефіцієнт *OSNR* і знижується коефіцієнт *BER* в кожному ОТр. Мінімізацію шумів можливо досягнути зменшенням кількості *OLAs* при заданому за Рек. *ITU-T G*.692 робочому затуханні ДП ($a_P^{ДП}$) та довжиною секції *OASs* (ℓ_{OAS}). Результати, що наведені в табл. 1, вказують на наявність структур *OASs* з гранично мінімальними коефіцієнтами *OSNR*.

Таблиця 1.

Типи ООВ	Параметри	*L OLAs*	*VL OLAs*	*UL OLAs*	Примітки
	ℓ_{OAS}, км	640	600	1280	
	$a_P^{ДП}$, дБ	22	33	44	
Рек. *ITU-T G*.692	$\ell_{ПД}$, км	80	120	160	*Corning: OB T (SSF G.652)* *Fujikura: DSM*-8/125 *(DSF G.653)*
	$\alpha_{ООВ}$, дБ/км	0,275			
	$N_{ВОП}$ / $n_{ДП}$	9/8	6/5	9/8	
Варіант 1 *NZ DSF* Рек. *ITU-T G*.655	$\alpha_{ООВ}$, дБ/км	0,24	0,22	0,24	*Lucent Technologies: AllWave; TrueWave* *Corning: LEAF; SMF* *Fujikura: SM*-10/125; *DSMNZ*-9/125
	$\ell_{ДП}$, км	≈91,4	150	≈183	
	$N_{ВОП}$ / $n_{ДП}$	8/7	5/4	8/7	
	Δ_{OSNR}, %	11	17	11	
Варіант 2 *NZ DSF*	$\alpha_{ООВ}$, дБ/км	0,205	0,165	0,206	Гранично мінімальні для *VL OLAs*
	$\ell_{ДП}$, км	≈107	200	213	
	$N_{ВОП}$ / $n_{ДП}$	7/6	4/3	7/6	
	Δ_{OSNR}, %	22	33	22	
Варіант 3 ООВ	$\alpha_{ООВ}$, дБ/км	0,172	0,11	0,172	Гранично мінімальні для *L* і *UL OLAs* Не досяжне для *VL OLAs*
	$\ell_{ДП}$, км	128	300	256	
	$N_{ВОП}$ / $n_{ДП}$	6/5	3/2	6/5	
	Δ_{OSNR}, %	33	–	33	

При застосуванні ООВ типу *NZ DSF* різних вендерів з коефіцієнтами затухання менш 0,275 дБ/км зменшується загальний рівень шумів (Δ_{OSNR}) в границях від 11 до 33%, що дозволяє зробити висновок про якісне поліпшування коефіцієнту *BER* в кожному ОТр за рахунок трансформації структур секцій *OASs* лінійних трактів ВОСП СУ.

Література

1. Хмелев К.Ф. Основы фотонного транспорта. – Киев: Техніка. 2008. – 680 с.
2. Бердников О.М., Хмельов К.П. Застосування технології *WDM* на телекомунікаційних мережах / Збірник наукових праць ВІТІ НТУУ “КПІ”. – 2003. – № 3. – с. 5…11.

УДК 621.38

РОЗШИРЕННЯ ФУНКЦІОНАЛУ ПРИСТРОЇВ TUYA SMART З ВИКОРИСТАННЯМ МОВИ ПРОГРАМУВАННЯ PYTHON

Голяткін А. О., Мошинська А. В.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: holiatkin_andrii@ukr.net

EXTENDING THE FUNCTIONALITY OF TUYA SMART DEVICES USING THE PYTHON PROGRAMMING LANGUAGE

Prospects for the development of the Internet of Things industry are considered. Ways to expand the functionality of smart devices from the Tuya Smart company are also considered. In addition, a solution to the practical use of IoT devices in the conditions of modern war in Ukraine is proposed.

Інтернет речей (Internet of Things, IoT) - це технологія, що з'єднує різні пристрої, які можуть обмінюватися даними без необхідності людського втручання. Ця технологія розвивається дуже швидко і очікується, що кількість підключених до Інтернету речей зросте з 26,66 млрд в 2019 році до 75,44 млрд в 2025 році, а світові витрати на IoT досягнуть 1,1 трильйона доларів США. (за даними Statista). Проте, розширення функціоналу розумних пристроїв є актуальною проблемою, оскільки вони часто не можуть виконувати всі завдання, які бажають користувачі [1, 2].

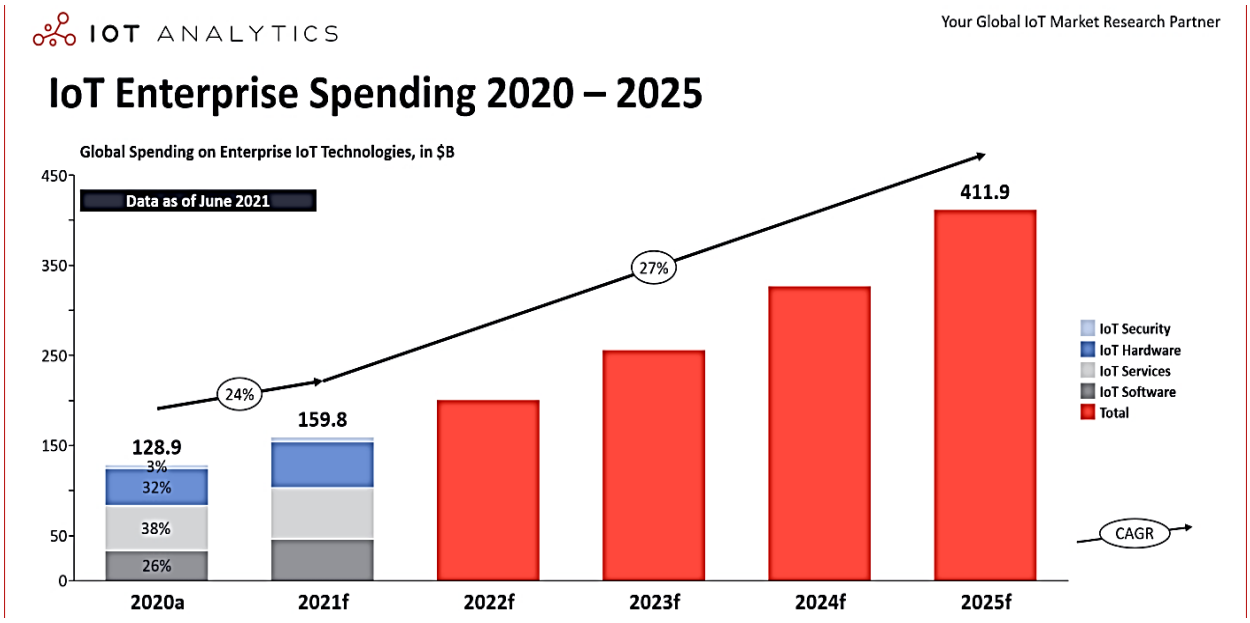


Рис.1. «IoT Enterprise Spending 2020-2025 according to IoT Analytics data».

У зв’язку з повномасштабним вторгненням країни агресора 2022 рік став наочним прикладом, чому в Україні важливо розвивати технології Інтернету речей та розширювати функціонал застосування не тільки для мирних побутових та індустріальних цілей, але й для безпеки життя громадян країни у воєнному стані. Особливу увагу в даному питанні треба приділити технологіям, які забезпечують інформацією миттєвого реагування, стають інклюзивними та допомагають людям з певними вадами здоров’я.

Прикладом практичного застосування пристрою IoT з розширеним функціоналом може бути розробка програми на Python, яка б дозволяла змінювати колір розумної LED-лампи в залежності від наявності або відсутності повідомлення про повітряну тривогу на території області користувача.

Дане програмне забезпечення змогло б допомогти людям з вадами слуху, які фізично не можуть чути сигнал повітряної тривоги, або людям похилого віку, які погано користуються смартфоном. Це дуже важливо в сьогоднішніх реаліях, адже своєчасне реагування людини на небезпеку може зберегти їй життя.

Однією з компаній, яка пропонує рішення поставленої задачі є Tuya Smart - один з провідних світових постачальників платформ AI (Artificial intelligence) + IoT і продуктів для розумного будинку. Tuya Smart пропонує широкий асортимент продуктів для розумного будинку, таких як розумні лампочки, вимикачі, розетки, камери тощо. Розумні пристрої від Tuya Smart мають великий потенціал для розширення функціоналу, адже можуть додаватися до хмарної платформи Tuya IoT Platform, яка об’єднує розумні пристрої та дозволяє користувачам керувати ними з будь-якої точки світу за допомогою своїх смартфонів. Платформа проста у використанні та може бути інтегрована з різними екосистемами розумного будинку, такими як Amazon Alexa, Google Assistant та IFTTT [3].

Платформа Tuya Smart підтримує широкий спектр протоколів зв’язку, таких як Wi-Fi, Bluetooth, Zigbee і Z-Wave, що робить її сумісною з смарт-пристроями від різних виробників. Також вона надає API (*Application Programming Interface)*, який дозволяє розробникам інтегрувати свої смарт-пристрої з платформою та розширювати їх функціональність. API доступний різними мовами програмування, такими як Python, Java і Node.js [4].

Основною перевагою мови програмування Python перед іншими мовами програмування є наявність великої кількості різних бібліотек та сторонніх модулів з широким спектром можливостей [5]. Однією з таких бібліотек є бібліотека tuya_iot - інструмент, що дозволяє керувати пристроями Tuya Smart з використанням мови програмування Python. Бібліотека tuya_iot базується на протоколі Tuya API, що дозволяє здійснювати зв'язок між Python та підключеними до мережі Tuya Smart пристроями. За допомогою неї можна здійснювати різноманітні операції з ними: вмикання та вимикання пристрою, зміна кольору світла, регулювання яскравості світла, тощо [4, 6].

Для роботи з бібліотекою потрібно мати додаткові дані, такі як ідентифікатори пристроїв та ключі API. Їх можна отримати з додатку Tuya Smart або відповідної хмарної платформи [4, 6].

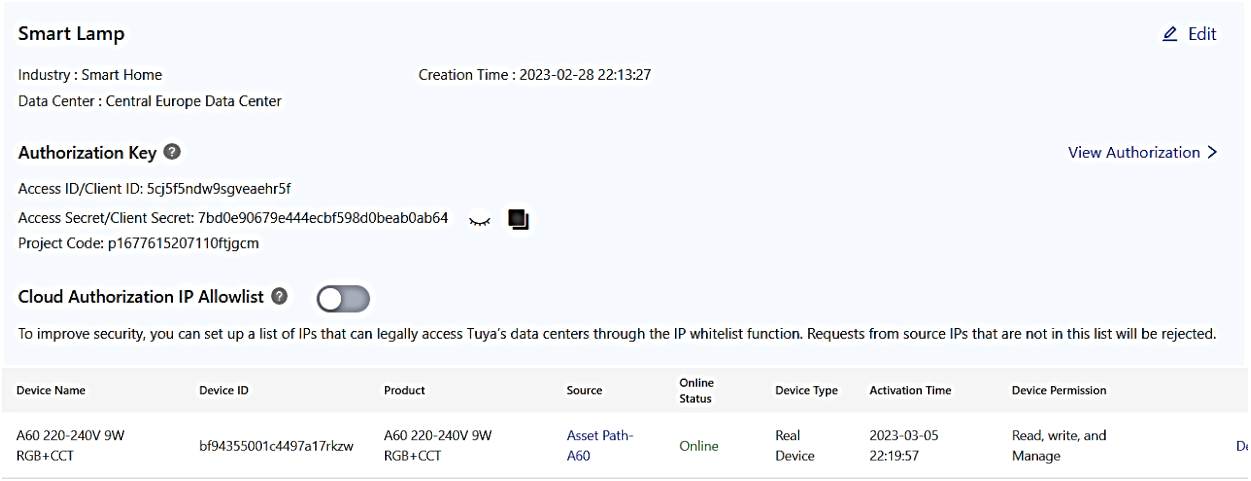


Рис.2. Дані про проект на платформі Tuya IoT Platform.

Бібліотека tuya_iot є досить популярним інструментом для розробки різноманітних IoT-проектів з використанням мови програмування Python для роботи з різними типами пристроїв, такими як розумні LED-лампи, розетки, димові детектори, тощо. Вона має ряд функцій для керування пристроями Tuya Smart, наприклад, такі як ініціалізація з'єднання (login(), connect(), та get_access_token()), відправка команд(метод post() та device_control()), отримання даних (метод get()) та інші [4, 6].

Для користувачів, які мають певний досвід роботи з Python, це може стати потужним інструментом для розширення функціоналу та налаштування пристроїв Tuya Smart під свої потреби.

Література

1. Marlene Greenfield, Number of connected devices worldwide from 2018 to 2025. URL: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
2. Philipp Wegner, Global IoT spending to grow 24% in 2021, led by investments in IoT software and IoT security. URL:https://iot-analytics.com/2021-global-iot-spending-grow-24-percent/
3. Офіційний сайт компанії Tuya Smart. URL: https://www.tuya.com/
4. Хмарна платформа Tuya IoT Platform. URL: https://iot.tuya.com/
5. Офіційний сайт мови програмування Python. URL: https://www.python.org/
6. Документація фреймворку Tuya IoT Python SDK. URL: https://github.com/tuya/tuya-iot-python-sdk

УДК 004.9

АНАЛІЗ ПРОБЛЕМ ПРИ РЕАЛІЗАЦІЇ ТЕХНОЛОГІЇ ІНДУСТРІАЛЬНОГО ІНТЕРНЕТА РЕЧЕЙ

[1]Кононова І. В., [1]Самусь Д.В., [2]Самусь Г.І.
[1]Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
[2]Конотопський інститут Сумського державного університету
E-mail: dimasamus99@gmail.com

ANALYSIS OF PROBLEMS IN THE IMPLEMENTATION OF INDUSTRIAL INTERNET OF THINGS TECHNOLOGY

The article examines the essence and aspects that need to be taken into account when considering the Internet of Things, in particular, attention is paid to the importance of industrial IIoT. The main problems of IoT technologies are identified.

На сьогодні, в епоху цифрової революції 4.0 важливу роль в житті людини відіграє застосування Інтернету речей (IoT). Першою метою впровадження IoT шляхом оснащення всіх об'єктів у світі мініатюрними пристроями ідентифікації було перетворення повсякденного життя, внесення до нього більшого комфорту, упорядкованості та прогнозованості [1].

Слід зазначити наступні аспекти, які потрібно враховувати під час впровадження рішень IoT: системний, інтелектуальний, інформаційний, проектний, управлінський. Так, системний аспект дозволяє розглядати систему, технологію чи процес із системних позицій. Інтелектуальний аспект вимагає поділу IoT-пристроїв за функціями на «розумні» та «інтелектуальні». Інформаційний аспект дозволяє розглядати IoT як міжмережеву взаємодію фізичних пристроїв (підключених чи інтелектуальних пристроїв). Проєктний аспект дозволяє розглядати схему IoT як інформаційну конструкцію. Управлінський аспект вимагає розглядати IoT як систему із сетецентричним або субсидіарним управлінням.

Важливе значення має IoT для моніторингу оточуючого середовища, управління інфраструктурою, в медицині, в будівництві, в інтеграції засобів зв'язку, управлінні та обробці інформації [1]. Загалом можна виділити сім галузей застосування технології IoT (рис.1), а саме: людина, будинок, офіс, підприємство, виробничий об’єкт, місто, зовнішній параметр.

Рис.1. Галузі застосування технології IoT.

Глобальним сегментом IoT для корпоративного (галузевого) застосування є індустріальний Інтернет речей (Industrial Internet of Things, IIoT) – Інтернет речей для корпоративного або галузевого використання – система об'єднаних комп'ютерних мереж та підключених промислових об'єктів із вбудованими датчиками та програмним забезпеченням для збору та обміну даними, з можливістю віддаленого контролю та управління в автоматизованому режимі, без участі людини [2].

Для позначення вужчого промислового сегменту IoT застосовується термін «промисловий Інтернет речей». Впровадження IIoT в обробній промисловості може призвести до збільшення ефективності виробництва, що стане поштовхом до четвертої промислової революції (Industry 4.0) [2]. Отже, IIoT – це еволюція розподіленої системи управління (DCS), яка дозволяє підвищити рівень автоматизації за рахунок використання хмарних обчислень для уточнення та оптимізації управління процесом.

IIoT використовує технології кібербезпеки, хмарні обчислення, граничні обчислення, мобільні технології, міжмашинну взаємодію, 3D-друк, передову робототехніку, аналіз великих обсягів даних, IoT, технологію RFID та когнітивні обчислення. Виділимо п'ять найважливіших з них: 1. Кіберфізичні системи –інформаційно-технологічна концепція, що передбачає інтеграцію обчислювальних ресурсів у фізичні процеси [3]. 2. Хмарні обчислення дозволяють надавати IT-послуги, ресурси при цьому завантажуються та вилучаються без прямого підключення до сервера [4]. 3. Крайові обчислення – парадигма розподілених обчислень, що наближає комп'ютерне сховище даних до місця, де вони потрібні [5]. 4. Аналітика великих даних – процес вивчення великих і різноманітних наборів даних або великих обсягів даних [6]. 5. Штучний інтелект та машинне навчання [7].

Системи IIoT часто сприймаються як багаторівнева модульна архітектура цифрових технологій. Рівень пристрою визначається фізичним компонентом: CPS, датчиком чи машиною. Мережевий рівень включає фізичні мережеві шини, хмарні обчислення та протоколи зв'язку, що агрегують та транспортують дані на сервісний рівень. Сервісний рівень складається з додатків, які працюють з даними та об'єднують їх у інформацію, що відображається на панелі приладів драйвера.

Для того, щоб IoT впровадити в більш широке використання, необхідно вирішити низку проблем. Деякі з цих проблем мають технічний характер, інші – суто структурний. Наприклад, користувачі повинні почати довіряти системам, що працюють на основі IoT, а компаніям необхідно при прийнятті рішень використовувати підходи на основі цифрових даних.

Розглянемо основні проблеми при реалізації технологій IIoT:

1. Сумісність пристроїв. Здатність пристроїв та систем IIoT працювати спільно має вирішальне значення для реалізації всіх можливостей IIoT - додатків. Прийняття відкритих стандартів є одним із способів забезпечення сумісності.

2. Конфіденційність. У більшості користувачів викликають занепокоєння проблеми конфіденційності особистих даних, що збираються

мільярдами пристроїв, та незаконного їх використання, організації непокоїть можливість незаконного доступу до комерційної конфіденційної інформації.

3. Захист даних. Організації, що збирають дані з мільярдів пристроїв, повинні мати можливість захистити ці дані від несанкціонованого доступу бо поширення інформаційних технологій на нові пристрої створює набагато більше потенційних вразливостей.

4. Захист інтелектуальної власності. Щоб розкрити величезний потенціал IoT, потрібно чіткіше розмежувати права та обов'язки учасників правовідносин, що виникають у зв'язку із застосуванням технологій IoT, і визначити, які права поширюються на дані, створювані різними підключеними пристроями.

Усі вищезазначені проблеми пов’язані з питаннями безпеки.

Отже, промисловий Інтернет речей - це мережа пристроїв, які пов'язані між собою за допомогою комунікаційних технологій. Одним із складних завдань у розвитку концепції Інтернет речей (IoT) у багатьох додатках є складні проблеми забезпечення інформаційної безпеки у широкому спектрі захисту від загроз зловмисника. Ці проблеми особливо актуальні, оскільки прогнозується зростання потреби користувачів в IoT.

Безпека інтернету речей передбачає захист інтернет-пристроїв та мереж, до яких вони підключені, від онлайн-загроз та зломів. Це досягається шляхом виявлення, моніторингу та усунення потенційних вразливостей безпеки на пристроях.

Література

1. Industrial Internet of Things Platform Comparison // M&S Consulting : [site]. 2016. 08 Febr. URL: https://www.mandsconsulting.com/industrial-iot-platform-comparison/ (date of access: 21.02.2023).
2. Industrial Internet of Things, IioT. URL: https://www.it.ua/knowledge-base/technology-innovation/promyshlennyjinternet-veschej (the date of access: 20.02.2023).
3. The industrial internet of things (IIoT): An analysis framework / H. Boyes [et al.] // Computers in Industry. 2018. Vol. 101. P. 1–12. URL:https://doi.org/10.1016/j.compind.2018.04.015. (date of access: 16.02.2023).
4. Frankenfield J. Cloud Computing // Investopedia : [site]. 2020. 28 July. URL: https://www.investopedia.com/terms/c/cloud-computing.asp (date of access: 22.03.2023).
5. Hamilton E. What is Edge Computing: The Network Edge Explained // Cloudwards : [site]. 2018. 27 Dec. URL: https://www.cloudwards.net/what-is-edge-computing/ (date of access: 11.02.2023).
6. Chai W., Labbe M., Stedman C. Big data analytics // SearchBusinessAnalytics.com : [site]. 2021. URL: https://searchbusinessanalytics.techtarget.com/definition/big-data-analytics (date of access: 3.03.2023).
7. Artificial Intelligence (AI) // Techopedia: [site]. 2020. 27 March. URL: https://www.techopedia.com/definition/190/artificial-intelligence-ai (date of access: 15.03.2023).

УДК 621.391.6

ДОСЛІДЖЕННЯ IOT M2M-ПРОТОКОЛІВ ДЛЯ ЗНИЖЕННЯ ЙМОВІРНОСТІ ДТП

Бабич І.О., Осипчук С.О.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: van.ba0611@gmail.com

IOT M2M PROTOCOLS RESEARCH TO REDUCE ROAD ACCIDENT PROBABILITY

This report provides the use of advanced Machine-to-Machine (M2M) communication technologies for the automotive industry. The report covers the latest developments in M2M technologies such as 5G, which is expected to revolutionize the way cars communicate with each other and with the surrounding infrastructure. Additionally, the report shows benefits of M2M technologies for the automotive industry, specifically improved safety.

Проблема, що вирішується. Автомобільні дорожньо-транспортні пригоди (ДТП) є однією з найбільш поширених причин загибелі людей у світі, зокрема в Україні. Статистика свідчить [1], що за 2021 рік, загалом в країні зареєстровано 24521 ДТП, в яких загинуло 3238 людина, та було травмовано 29738 осіб. Отже, зменшення ймовірності виникнення ДТП з метою збереження людських життів та зменшення ймовірності летального результату ДТП у світі та в Україні є актуальним завданням.

Постановка завдання. Зменшити ймовірність виникнення ДТП та летального результату ДТП.

Шляхи вирішення завдання. Поставлене завдання можна вирішити різними способами, а саме: системним обмеженням швидкості руху транспортних засобів (ТЗ) до безпечного на законодавчому рівні; конструктивною організацією доріг та її елементів; впровадженням технічних рішень взаємодії ТЗ у русі, тощо.

Одним із технічних рішень вирішення поставленого завдання є організація комунікації між транспортними засобами, які перебувають у русі, з метою збору та обміну інформацією між ТЗ, і централізованого чи децентралізованого прийняття рішень транспортними засобами в реальному режимі часу щодо необхідності реагування ТЗ на обставини, що склалися в кожен момент часу у процесі руху.

Комунікація між ТЗ може бути організована з використання протоколів Інтернету Речей (Internet of Things, – IoT [2]), та міжмашинного зв’язку, відомого як M2M-комунікації (англ. M2M – Machine-to-Machine Communications, [3]).

Міжмашинний зв’язок використовується для автоматизованої передачі даних та вимірювань між механічними або електронними пристроями. Ключовими компонентами системи M2M є безпроводові пристрої із вбудованими датчиками або RFID, безпроводові комунікаційні мережі стільникового зв’язку, Wi-Fi, ZigBee, WiMAX, WLAN, а також проводові

інфокомунікаційні мережі [4]. На рис. 1 зображено архітектуру інфокомунікаційної M2M мережі IoT в контексті автотранспорту і ТЗ [5].

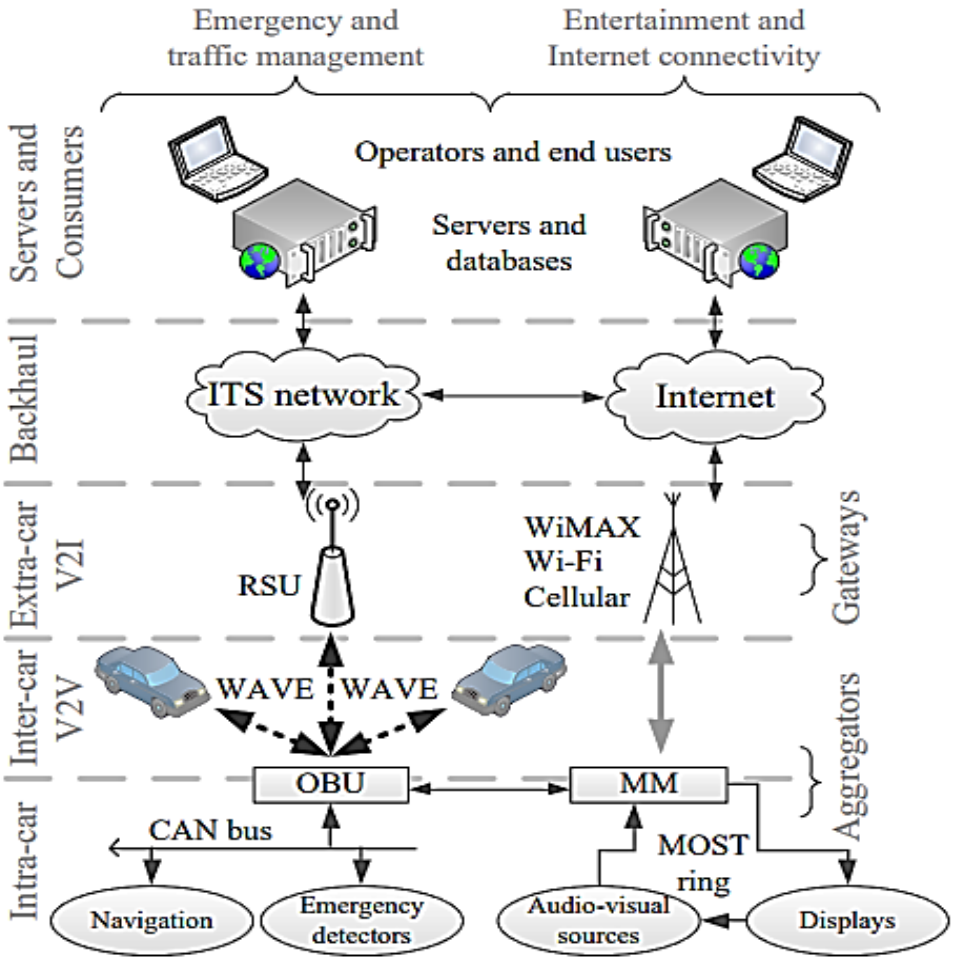


Рис. 1. Архітектура мережі M2M в контексті автотранспорту.

Варто відзначити, що достовірність та своєчасність передавання інформації є надзвичайно важливими характеристиками для організації безпроводового M2M зв’язку. Мережі з низькою затримкою, такі як 5G, покращують M2M зв’язок між ТЗ та пристроями, і забезпечують безперебійний потік інформації для врахування невизначеностей дорожнього руху, включаючи аварії та дорожні умови [6].

Можливі застосування M2M-протоколів в автомобільній промисловості:

1. Збір даних про рух ТЗ, взаємодія з мережами, іншими ТЗ та інфраструктурою навколо ТЗ [6]. Ці дані можуть використовуватися для аналізу стану дороги, передбачення можливих аварій та забезпечення більш ефективного руху ТЗ. Наприклад, збір даних про швидкість руху, погодні умови, гальмування та розгін, насиченість трафіку ТЗ можуть допомогти виявити небезпечні ділянки дороги та розробити заходи для зменшення ризику ДТП.

2. Забезпечення комунікації між вузлами ТЗ для покращення безпеки руху. Наприклад, використання протоколів M2M може допомогти забезпечити зв'язок між системою автоматичного гальмування автомобіля.

Прикладом реалізації комунікації між вузлами ТЗ є колізійна система попередження (Collision Warning System, – CWS) [7-8]. CWS може виявити небезпеку зіткнення та надіслати відповідний сигнал водієві та системі гальмування, що допомагає уникнути ДТП та зменшити число травмованих.

За даними Європейської асоціації автовиробників (ACEA), 40,5% нових легкових автомобілів, що були зареєстровані в Європі, мали системи екстреного гальмування з датчиком перешкод (Autonomous Emergency Braking, – AEB), що є однією з видів систем CWS.

IoT M2M протоколи. Один з можливих протоколів, які можуть використовуватись у CWS, – CAN (Controller Area Network). CAN – це промисловий стандарт протоколу, який використовується для обміну даними між компонентами автомобільної системи, включаючи сенсори, контролери та інші пристрої. CAN дозволяє швидкий та надійний обмін даними в реальному часі та є одним з найбільш поширених протоколів в автомобільній промисловості.

Інші протоколи, які можуть використовуватись у CWS, включають Bluetooth, Wi-Fi, Zigbee та інші безпроводові протоколи, які дозволяють передавати дані між компонентами системи без використання кабелів. Наприклад, система CWS може використовувати Bluetooth для передачі даних між сенсорами, контролерами та іншими пристроями в автомобілі.

Зменшення ймовірності ДТП. Згідно зі звітом NHTSA про статистику аварій з участю автотранспорту за 2019 рік [9], з них 8,2% (або більше 3 000 аварій) відбулися через зіткнення з перешкодою, яку автомобіль міг запобігти за допомогою системи попередження про зіткнення. Дослідження NHTSA також показує, що встановлення M2M системи попередження про зіткнення в автомобілях, яка працює з використанням радару або камери, може знизити кількість аварій на 20% [9].

Висновок. Використання M2M-протоколів в автомобільній промисловості допомагає якісно та кількісно зменшити кількість ДТП, та поліпшити безпеку на дорогах.

Література

1. МВС України: https://patrolpolice.gov.ua/statystyka/
2. "IoT for All." [Online]. Available: https://www.iotforall.com/
3. Gartner: M2M, report – https://www.gartner.com/en/information-technology/glossary/machine-to-machine-m2m-communications
4. Yang Cao, Tao Jiang, Zhu Han. A Survey of Emerging M2M Systems: Context, Task, and Objective / IEEE Internet of Things Journal. – 2016.
5. M2M Communications in Vehicular Networks https://bit.ly/3M5Exo8
6. IEEE 1609.4, "Стандарт IEEE для бездротового доступу в транспортних середовищах (WAVE)-багатоканальна робота", IEEE Std DOI: 10.1109/IEEESTD.2011.5712769, 2011.
7. J. Xu, Y. Wang, and Y. Liu, "A review of intelligent collision warning systems in vehicles," IEEE Transactions on Intelligent Transportation Systems, vol. 15, pp. 2966-2979, 2014.
8. Y. Zhang and C. Cheng, "A review of recent advances in collision warning systems, "Transportation Research Part C: Emerging Technologies, vol. 69, pp. 507-523, 2016.
9. Звіт Національного управління безпеки руху на дорогах США (NHTSA) https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/813060

УДК 621.39

ВИКОРИСТАННЯ ЦИФРОВИХ ПІДПИСІВ І СЕРТИФІКАТІВ ДЛЯ БЕЗПЕКИ ТРАНЗАКЦІЙ І ПІДТВЕРДЖЕННЯ СПРАВЖНОСТІ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

Григоренко О.Г., Реута Г.В.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: olenagri@ukr.net, glebreuta14@gmail.com

DIGITAL SIGNATURES AND CERTIFICATES USING FOR SECURE TRANSACTIONS AND CONFIRMATION OF THE ELECTRONIC DOCUMENTS AUTHENTICITY

Analyzed features of digital signatures and certificates and the advantages of their use in various areas of modern life, which allows safe transactions on the Internet and confirm the authenticity of electronic documents.

Проаналізовані особливості цифрових підписів та сертифікатів та переваги їх використання в різних сферах сучасного життя, що дозволяє безпечно проводити транзакції в мережі Інтернет та підтверджувати справжність електронних документів.

Цифрові підписи та сертифікати використовуються у різних сферах нашого життя. «Зелене світло» для широкого застосування електронних документів та цифрового підпису в Україні дали Закон “Про електронні документи та електронний документообіг” та Закон “Про ЕЦП” [1,2]. В Україні використання цих технологій є надзвичайно актуальним через війну, а раніше локдаун.

Цифровий підпис - вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача [2,4,5]. Електронний цифровий підпис (ЕЦП) накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа. Ілюстрація цифрового підпису показана на рис.1.

Рис.1. Ілюстрація цифрового підпису даних [7].

Цифровий підпис складається з двох частин:

перша — відкрита для тих сторін, що обслуговують програмне забезпечення, яке використовує та допомагає складати електронні документи, відправляє та отримує електронні документи, — ця частина дозволяє таким сторонам ідентифікувати особу;

друга — секретна частина створюється лише власником підпису, це є пароль власника, яким він користується, щоб створити електронний цифровий підпис та потім підписувати ним електронні документи.

Гарантії цифрового підпису забезпечуються його особливостями [3]:

- **Автентичність.** Підтверджується особа, яка підписала документ.

- **Цілісність.** Вміст не змінено або не підроблено після того, як на ньому поставлено цифровий підпис.

- **Неможливість відмови.** Підтверджує для всіх сторін походження підписаного вмісту. Відмова – це заперечення автором підпису своєї причетності до підписаного вмісту.

- **Нотаріальне засвідчення.** Підписи у файлах, наприклад, Microsoft Word, Microsoft Excel або Microsoft PowerPoint із позначкою часу від надійного сервера позначок часу за певних умов прирівнюються до нотаріального засвідчення.

Сертифікат — це цифровий документ, який використовується для підтвердження справжності цифрового підпису. Він видається Центром сертифікації і містить інформацію про власника підпису та ключ, до якого він був створений. Сертифікат може бути використаний для перевірки справжності та цілісності даних, які були створені за допомогою відповідного цифрового підпису.

Цифрові сертифікати використовуються для перевірки організації або окремого користувача, а також для аутентифікації веб-сайту постачальника і встановлення зашифрованого з'єднання для обміну конфіденційними даними. Якщо цифровий сертифікат відповідає стандартній структурі, то його може прочитати та зрозуміти будь-яка система незалежно від того, ким він був виданий. X.509 є стандартом для інфраструктури відкритих ключів (PKI - public key infrastructure) для керування цифровими сертифікатами.

Найпоширеніші приклади використання цифрових підписів та сертифікатів (ЦПС) у різних галузях включають: електронну комерцію (для безпечної аутентифікації електронних платежів та забезпечення конфіденційності та цілісності електронних транзакцій між різними сторонами), банківський сектор, державну та муніципальну сфери, медичну сферу (для підписання та обміну медичними документами та рецептами), корпоративну сферу, Інтернет-безпеку (для перевірки справжності та цілісності веб-сайтів та захисту користувачів від фішингу та інших типів шахрайства), інтелектуальну власність (для захисту авторських прав і патентів).

На онлайн-платформі державних послуг ДІЯ за допомогою ЕЦП можна отримати послуги щодо отримання грантів для розвитку малого та середнього бізнесу, електронний кабінет пенсійного фонду, електронний кабінет водія тощо [6].

Найбільш поширеними є три алгоритми цифрового підпису - Digital Signature Algorithm (**DSA)**, Rivest-Shamir-Adleman (**RSA**) і Elliptic Curve Digital Signature Algorithm (**ECDSA**). Всі три алгоритми містять механізми створення та перевірки цифрових підписів і функціонують **на основі**

асиметричного шифрування з використанням відкритих ключів. Операції генерації ключа та перевірки вимагають шифрування і дешифрування ключів.Також була представлена розширена криптосистема цифрового підпису Меркле (XMSS), яка має пряму секретність та стійкість до криптоаналізу із використанням квантових комп'ютерів [7].

Алгоритм DSA базується на складності обчислень дискретних логарифмів. Можливості алгоритму DSA обмежуються формуванням та перевіркою цифрового підпису. RSA є найбільш поширеним алгоритмом і може використовуватися не тільки для роботи з цифровими підписами, а також для шифрування повідомлення. DSA працює швидше, ніж RSA, в якості підпису для цифрового документа. Алгоритм RSA краще підходить для ситуацій, коли крім вимог підпису і перевірки електронних документів необхідне ще й шифрування повідомлень. Алгоритм RSA базується на двох математичних компонентах: модульній арифметиці і задачі факторизації великих цілих чисел. ECDSA поступово замінює RSA тому, що ECDSA може використовувати набагато менші розміри ключа при такому ж рівні безпеки і вимагає значно менших об'ємів обчислень, ніж RSA.

Надзвичайно важливим є використання позначок часу при застосуванні ЕЦП, бо їх відсутність призводить до критичної вразливості і дозволяє реалізувати атаки на ЕЦП [7]. Це пов'язано з особливостями застосування ЕЦП, щодо документів, термін дії яких перевищує термін дії ЕЦП. Валідність таких документів перевіряється тільки на момент підпису. Прикладом таких документів є подача електронної звітності.

Перераховані вище особливості електронного цифрового підпису є ефективним інструментом забезпечення інформаційної безпеки на всіх рівнях інфраструктури суспільства та держави. Окрім цього перехід до електронного документообігу дозволяє зберігати ліси, зменшувати кількість підприємств з виробництва паперу, що призводить до енергозбереження та захисту довкілля в результаті.

Література

1. Закон України від 22.05.2003 р. №851-IV «Про електронні документи та електронний документообіг».
2. Закон України від 22.05.2003 р. №852-IV «Про електронний цифровий підпис».
3. https://support.microsoft.com/uk-ua/office/%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D1%96-%D0%BF%D1%96%D0%B4%D0%BF%D0%B8%D1%81%D0%B8-%D1%82%D0%B0-%D1%81%D0%B5%D1%80%D1%82%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%82%D0%B8-8186cd15-e7ac-4a16-8597-22bd163e8e96
4. https://online.dtkt.ua/2012/20/50377
5. Цифровий електронний підпис // Юридична енциклопедія : [у 6 т.] / ред. кол.: Ю. С. Шемшученко (відп. ред.) [та ін.]. — К. : Українська енциклопедія ім. М. П. Бажана, 2004. — Т. 6 : Т — Я. — 768 с. — ISBN 966-7492-06-0.
6. https://pravokator.club/news/elektronnyj-tsyfrovyj-pidpys-osoblyvosti-vykorystannya/
7. https://uk.wikipedia.org/wiki/%D0%95%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B8%D0%B9_%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B8%D0%B9_%D0%BF%D1%96%D0%B4%D0%BF%D0%B8%D1%81

УДК 621

КОНФІДЕНЦІЙНІСТЬ ДАНИХ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ І ЗАСОБИ ЇЇ ЗАБЕЗПЕЧЕННЯ

Григоренко О.Г., Голуб О.С.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: olenagri@ukr.net, soupjhoney@gmail.com

DATA CONFIDENTIALITY IN INFORMATION COMMUNICATION NETWORKS AND MEANS OF ITS ENSURING

The current issue of data confidentiality in the network is considered and the main means of its provision are analyzed. This contributes to the safe transmission, processing and storage of data in the face of growing potential threats in cyberspace

Розглянуто актуальне питання конфіденційності даних в мережі та проаналізовані основні засоби її забезпечення. Це сприяє безпечній передачі, обробці та зберіганню даних при зростанні потенційних загроз в кіберпросторі

В сьогоднішньому світі, коли загальнодоступна мережа Інтернет використовується для обміну важливими даними, забезпечення конфіденційності даних є актуальною задачею для будь-якої інформаційної системи. У зв'язку з цим, важливим є проаналізувати засоби забезпечення конфіденційності даних в інфокомунікаційних мережах, визначити їх особливості.

Конфіденційність запобігає розкриттю інформації неавторизованим особам, ресурсам або процесам. Тому конфіденційність даних в кіберпросторі потрібно забезпечувати при їх зберіганні, обробці та під час передачі інфокомунікаційною мережею.

Поняття конфіденційної інформації включає дані, захищені від несанкціонованого доступу для гарантування безпеки окремій особі або організації. Конфіденційну інформацію можна розділити на три типи:

- персональна інформація - це особиста інформація, а саме дані, за допомогою яких можна визначити особистість людини. Це такі дані як паспортні дані, медичні записи, номера банківських карток, фінансова інформація;
- ділова інформація - це інформація, яка у разі оприлюднення може створити проблеми для організації. До таких даних відносяться торговельні секрети, плани придбання, фінансові дані, інформація споживача;
- секретна інформація - це інформація, що належить державним органам, засекречена через високий рівень конфіденційності.

Компанії, організації зазвичай обмежують доступ, щоб гарантувати, що тільки уповноважені особи можуть використовувати дані або інші мережні ресурси. Наприклад, програміст не повинен мати доступ до особистої інформації всіх співробітників. Також в компаніях потрібно навчати співробітників кращим методам захисту конфіденційної інформації, щоб

захистити їх та організацію від атак. Основні засоби, які використовуються для забезпечення конфіденційності, включають шифрування даних, аутентифікацію і контроль доступу, політики та процедури щодо кібербезпеки. безпечні протоколи (SSH, SSL/TLS, IPsec) [4], використання VPN (Virtual Private Network) (рис.1).

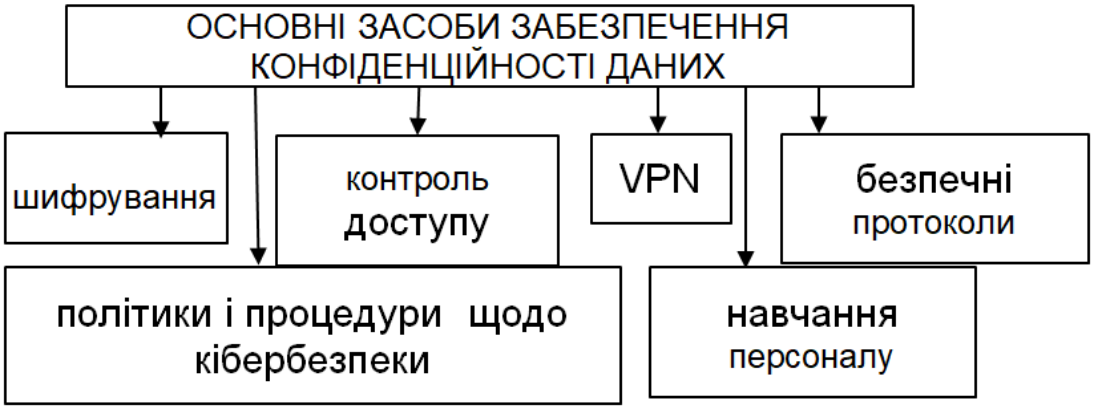


Рис.1 Основні засоби забезпечення конфіденційності

Шифрування перетворює дані таким чином, щоб неавторизована третя сторона не змогла їх прочитати [1]. Для шифрування використовуються математичні алгоритми, надійність яких напряму залежить від надійності ключа. Чим складніший ключ, тим більш безпечний алгоритм. Керування ключами є важливою частиною цього процесу. Всі сучасні криптографічні алгоритми містять обов'язкові процедури керування ключами. На практиці більшість атак на криптографічні системи спрямовані на систему керування ключами, а не на сам криптографічний алгоритм.

Контроль доступу визначає ряд схем захисту, які запобігають несанкціонованому доступу до комп'ютера, мережі, бази даних або інших ресурсів даних. Концепція AAA (Authentication, Authorization, Accounting) включає в себе три служби безпеки: аутентифікація, авторизація та облік. Ці служби забезпечують основну структуру контролю доступу.

Аутентифікація перевіряє особу користувача для запобігання несанкціонованому доступу [2]. Користувачі підтверджують свою особистість за ім'ям користувача або ідентифікатором. Аутентифікація вимагає, щоб користувач надав інформацію, яку він знає (наприклад, пароль), або/та підтвердив наявність чогось (наприклад, картка), або/та надав біометричну інформацію (наприклад, відбитки пальців). Найбільш популярною формою аутентифікації є використання паролів. Поєднання декількох типів аутентифікації відоме як багатофакторна аутентифікація, яка є більш безпечною і надійною завдяки неможливості для кіберзлочинців за короткий час зламати всі види захисту.

Авторизація визначає до яких ресурсів можуть отримати доступ користувачі, а також операції, які вони можуть виконувати. Деякі системи реалізують це за допомогою списку керування доступом або ACL (Access Control List). ACL визначає, чи має користувач певні привілеї доступу після проходження аутентифікації. Авторизація також може контролювати, коли,

тобто в який час, користувач має доступ до певного ресурсу.

VPN - це приватна мережа, яка використовує загальнодоступну мережу, зазвичай Інтернет, для створення безпечного каналу зв'язку [5]. VPN з'єднує за допомогою зашифрованого тунелю дві кінцеві точки, такі як два віддалених офіси, через Інтернет, щоб створити з'єднання.

Мережі VPN використовують IPsec - набір протоколів, розроблених для реалізації безпечних мережних сервісів. Сервіси IPsec забезпечують аутентифікацію, цілісність, контроль доступу та конфіденційність. За допомогою IPsec віддалені вузли можуть обмінюватися зашифрованою і перевіреною інформацією.

Для побудови політики інформаційної безпеки рекомендується окремо розглядати такі напрями захисту інформаційної системи [3] як захист об'єктів інформаційної системи; захист процесів, процедур і програм обробки інформації; захист каналів зв'язку різного виду; придушення побічних електромагнітних випромінювань і наведень; управління системою захисту.

Підсумовуючи, зазначимо, що забезпечення конфіденційності даних є на сьогодні надзвичайно актуальним питанням на тлі зростання потенційних загроз у кіберпросторі. Для цього застосовується комплекс технічних, організаційних, правових заходів. Аналіз особливостей засобів забезпечення конфіденційності показав, що основними є шифрування, використання безпечних протоколів та VPN. Особливу увагу організації приділяють контролю доступу та розробці політик і процедур щодо інформаційної безпеки. Також завжди треба враховувати людський фактор і регулярно проводити навчання з кібербезпеки для персоналу компанії і навчати новим технологіям захисту.

Література

1. Шифрування: типи і алгоритми/ [Електронний ресурс] – Режим доступу: https://hostpro.ua/wiki/ua/security/encryption-types-algorithms
2. Використання аутентифікації в мережі як способу виконання безпечних хмарних обчислень/ Григоренко О.Г., Полікарпова Ю.Г. // Збірник "Перспективи телекомунікацій" ПТ-2021. – К.: КПІ ім. Ігоря Сікорського, 2021. – С.44-46. ISSN (print) 2663-502X ISSN (online) 2664-3057 http://journals.uran.ua/ за посиланнями: http://conferenc.its.kpi.ua/proc/issue/archive, http://journals.uran.ua/ (ISSNonline 2664-305).
3. Системи забезпечення інформаційної безпеки/ [Електронний ресурс] / – Режим доступу: https://valtek.com.ua/ua/system-integration/security-control-system/integrated-security-systems/information-security-system-review.
4. WHAT IS SSL, TLS & HTTPS/ [Електронний ресурс] – Режим доступу:https://www.digicert.com/what-is-ssl-tls-and-https
5. Bacek / Принципы организации VPN // [Електронний ресурс] – Режим доступу: http://ciscotips.ru/vpn

UDC 621.391:006

PERSPECTIVE TRENDS OF TELECOMMUNICATION NETWORKS DEVELOPMENT BASED ON IMT-2030 CONCEPT

Triska N.R.
Educational and Scientific Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: ntriska@ukr.net

ПЕРСПЕКТИВНІ НАПРЯМКИ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ НА ЗАСАДАХ КОНЦЕПЦІЇ IMT-2030

Розглянуто перспективні напрямки розбудови сучасних телекомунікацій в контексті подальшого розвитку та впровадження базової концепції мобільного зв'язку – IMT. На основі програмних документів ITU-T проаналізовано основні засади розвитку сучасних та майбутніх телекомунікаційних систем на період до 2030 року (концепція IMT-2030). Відзначено важливість адаптації нових технологій та технічних рішень до існуючої інфраструктури телекомунікаційних мереж, а також необхідність забезпечення точної синхронізації для багатьох сучасних та майбутніх застосувань.

Ever-increasing demand for infocommunication services in very different fields of modern business and social life leads to the development of new technical concepts and solutions. As people communicate in high-definition video and gain more user experience with virtual reality, cloud gaming etc., the need for more bandwidth is growing. High-speed, low-latency device-to-device (D2D) interaction is also a very promising trend, especially for industrial processes automation and Internet of Things (IoT). New digital realities strongly influence the ways of learning, understanding and memorizing in different fields of science. It is important to note the steadily increasing role of users in the IT & Telecom market development: now the user experience shapes the technologies for personalized needs [1, 2].

On the other hand, new technical solutions should provide the sustainable interaction with existing resources and processes. So the role of standardization in the new technologies deployment is really important.

During the last decade the telecommunications development has been based on the IMT (International Mobile Telecommunications) concept defining the mobile broadband systems and corresponding network infrastructure. It reflects the ever-increasing role of mobile communications in the modern world. The emerging demand for new mobile services is one of the main driving factors in IT &Telecom now. IMT concept went through several stages of development (IMT-2000, IMT-Advanced, IMT-2020) and now the next stage – IMT-2030 – is actively discussed. So the development and standardization of IMT-2030 deployment scenarios will be in focus of telecom industry for the next years. The IMT-2020/2030 standardization activities are coordinated by the corresponding International

Communication Union sectors – ITU-R (radio technologies and interfaces) and ITU-T (network architecture, transport network, synchronization).

The capabilities of IMT systems are being continuously updated in line with user trends and technological developments. The current IMT-2020 concept (based on 5G mobile telecommunications standards) has introduced some promising technologies such enhanced mobile broadband (eMBB), ultra-reliable low-latency communications (URLLC) and massive machine-type communications (mMTC). Besides significantly enhancing the data rate and mobility provided in IMT-Advanced, IMT-2020 has introduced new advantages such as spectrum efficiency, latency, reliability, connection density, energy efficiency etc. to support emerging usage scenarios and applications.

IMT-2030 is expected to provide a revolutionary new user experience with connection speeds in the Terabits/s range per user and a whole new array of sensory information such as touch, taste and smell. New services and application trends for IMT towards 2030 and beyond are summarized in [1] and includes:

– Enabling services that help to steer communities and countries towards reaching the United Nations' Sustainable Development Goals (UN-SDGs);

– Customization of user experience based on the user-centric resource orchestration models;

– Community-driven networks and public–private partnerships as new models for future service provisioning;

– Development of products and technologies that innovate to zero will be promoted; for example, zero-waste and zero-emission technologies.

– Increasing role of artificial intelligence (AI) in different industry and social applications. The goal is to provide the access of AI to everyone, every business, every service anywhere anytime.

– The trend towards higher data rates will continue: peak data rates may approach Tera bits per second (Tbit/s) indoors, requiring large available bandwidths giving rise to (sub-) Tera hertz (THz) communications.

The technical base for implementation of the abovementioned tasks is being formed now. The three basic usage scenarios proposed for IMT-2020 – eMBB, mMTC and URLLC – will still remain relevant. At the same time, new promising use cases and applications (digital twin, cyber-physical systems, "mixed reality" – MR, industrial/service robots etc.) will require to develop and implement the various new technologies and solutions.

For example, the different solutions are proposed to enhance the radio interface such as advanced modulation, coding and multiple access schemes, advanced antenna technologies (e.g. E-MIMO) and holographic radio [1].

Extreme MIMO (E-MIMO) is further development of massive MIMO, which is widely deployed in IMT-2020 systems. It can be achieved by exploiting much larger antenna array, using new materials, applying new deployments and new tools, etc.

Holographic radio (HR**)** can be applied in some promising use cases, such as high-precision positioning and perception, smart factory and immersive media. It utilizes the spatially continuous electromagnetic aperture and interference

exploitation to enable spatial multiplexing and spectral multiplexing with pixelated ultra-high resolution. HR can make use of all available spatial dimensions to achieve benefits in terms of flexibility, spectral efficiency, delay, power consumption and complexity.

The important aspect of IMT-2020 (and future IMT-2030) systems deployment is the effective adaptation of the existing transport network infrastructure to new technical requirements [2, 3]. The main aspects of such adaptation has been summarized in ITU-T Recommendation G.8300 “Characteristics of transport networks to support IMT-2020/5G” [4] which defines:

- Relationship of 5G network architecture to transport network architecture;
- Operations, administration, and maintenance (OAM) requirements;
- Timing performance and time/synchronization distribution architecture;
- Survivability mechanisms.

All these issues will remain relevant as new solutions based on IMT-2030 concept are introduced. The use of data and algorithms such as artificial intelligence (AI) will play an important role, and technological complementarities are required to ensure that the technology innovations complement each other [1].

One of the most important aspects of new telecommunication technologies deployment has traditionally been synchronization issues [2, 3]. The precise synchronization will remain critical for many new application such as time-sensitive networking for automated vehicles, controlling robots in smart factories, high-precision positioning. Industrial devices, processes and future haptic applications will require strict timing synchronization with tight requirements for jitter. It should be considered in the respective ITU-T standards and in the new generations of synchronization equipment.

It is generally expected that IMT-2030-based networks will connect many devices, processes and humans to a global information grid cognitively, thereby offering new opportunities for various verticals. Future applications could allow users to feel material objects in holographic form, taste food samples in a kind of virtual reality, and even smell samples thanks to innovative digital scent technologies. But a lot of work should be done from the research & development to standardization and deployment of new technical decisions. All these activities should consider the need to adapt the new technologies, networks architectures as well as management and OAM tools with the existing network infrastructure.

References

1. REPORT ITU-R M.2516-0 Future technology trends of terrestrial International Mobile Telecommunications systems towards 2030 and beyond. – Electronic Publication: Geneva, 2022.
2. Тріска Н.Р. Актуальні завдання підготовки телекомунікаційних мереж до впровадження стандарту 5G. – Тринадцята Міжнародна науково-технічна конференція “Перспективи телекомунікацій” (ПТ-2019), 15-19 квітня 2019 р. Матеріали конференції. – ІТС НТУУ “КПІ”. – С. 131-133.
3. Тріска Н.Р. Питання впровадження стандарту 5G на базі існуючої інфраструктури мережі. – П’ятнадцята Міжнародна науково-технічна конференція “Перспективи телекомунікацій” (ПТ-2021), 12-16 квітня 2021 р. Матеріали конференції. – ІТС НТУУ “КПІ”. – С. 113-115.
4. ITU-T Recommendation G.8300 Characteristics of transport networks to support IMT-2020/5G (05/2020).

UDC 621.391.3

PRINTED DIPOLE ANTENNA FOR 2.4 GHZ FREQUENCY BAND

Trubarov I.V.
Educational and Scientific Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail:trubarov.i@gmail.com

ПРОЄКТУВАННЯ ТА ОПТИМІЗАЦІЯ ДРУКОВАНОЇ ДИПОЛЬНОЇ АНТЕНИ ДЛЯ ЧАСТОТНОГО ДІАПАЗОНУ 2,4 ГГЦ

Здійснено проєктування та оптимізацію симетричної дипольної антени діапазону 2,4 ГГц, виконаної за мікросмужковою технологією. Живлення антени здійснюється коаксіальним кабелем, що передбачає реалізацію симетрувального пристрою. 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 смузі робочих частот. В межах робочої смуги частот КСХ розрахованої антени знаходиться в діапазоні 1…1.2.

Printed microstrip antennas are widely used in communication systems due to their small dimensions, low cost and possibility to integrate an antenna with the device at the common printed circuit board (PCB). There is a large number of small-size antenna types and design techniques that can be used for their analysis and fabrication [1] – [3]. Among the microstrip radiating structures, patch antennas are often used. However, these antennas are not omnidirectional and typically have gain of 6…9 dB [4 – 7]. To obtain omnidirectional directivity pattern, dipole or monopole antenna structures should be used.

In this paper, a microstrip dipole antenna for 2.4 GHz band is designed and simulated using the finite-element method. The antenna to be designed shall operate in 2400…2483 MHz frequency range, and have uniform directivity pattern in one of the planes. The proposed antenna can be used in mobile ISM (Industrial, Scientific and Medical) band communication systems, such as Wi-Fi, Bluetooth or Zigbee applications. Thus, the operating frequency of the antenna was chosen to be f_0 = 2442 MHz, which is the center frequency of the operating band.

As a substrate for the antenna, FR4 laminate was used with the following parameters: dielectric constant ε_r = 4.4; thickness h = 1.5 mm; thickness of the top and bottom copper layers t = 0.020 mm; dissipation is defined by tan δ = 0.02.

The layout of the antenna is shown in Fig. 1. The antenna was designed so as to be fed by microstrip line or coaxial cable using SMA (SubMiniature version A) connector. Since a dipole antenna has balanced input, a balun is needed to convert unbalanced coaxial or microstrip input to balanced input of the antenna. In the presented antenna, tapered balun was used. Linear tapering was implemented due to its simplicity and pertinent transmission characteristics. To provide impedance matching, the dipole arms section, feed section and the balun were designed to have 50 Ω input impedance.

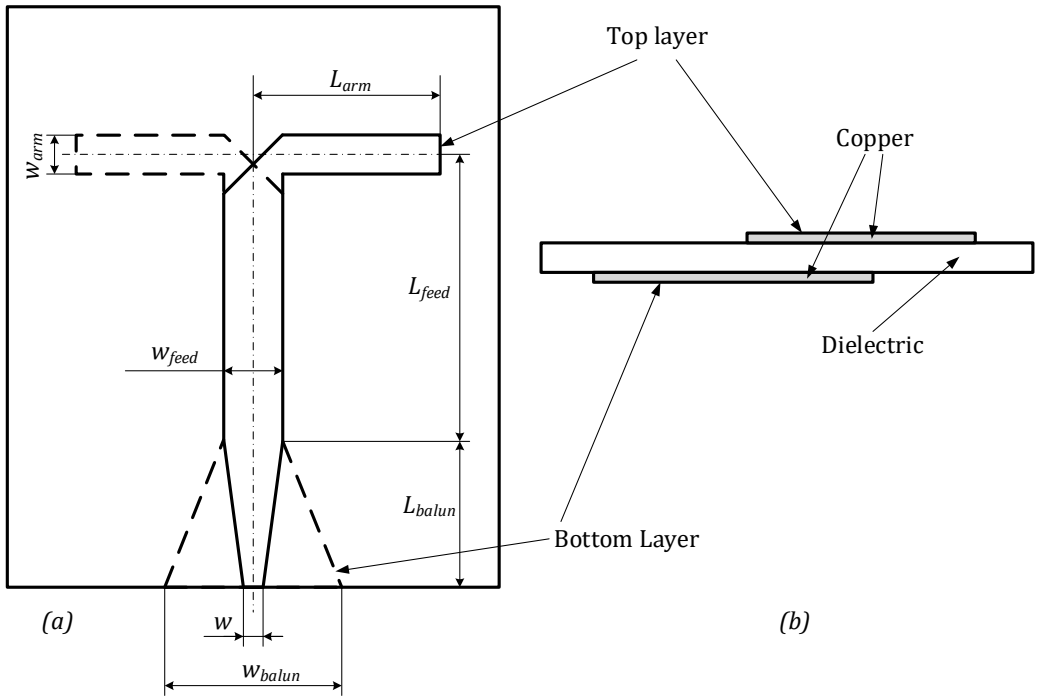


Fig. 1. Dimensions of a microstrip dipole antenna. (a) Antenna dimensions. (b) Side view of the antenna.

The theory and design approach for the selected antenna type are considered in [1] – [3]. The design procedure contained the following stages: analysis of the printed dipole section in order to match the resonant frequency and provide 50 Ω input with minimum value of reactance; design of the feeding section so as to provide impedance matching; design and optimization of the balun section; final simulation and optimization of the antenna.

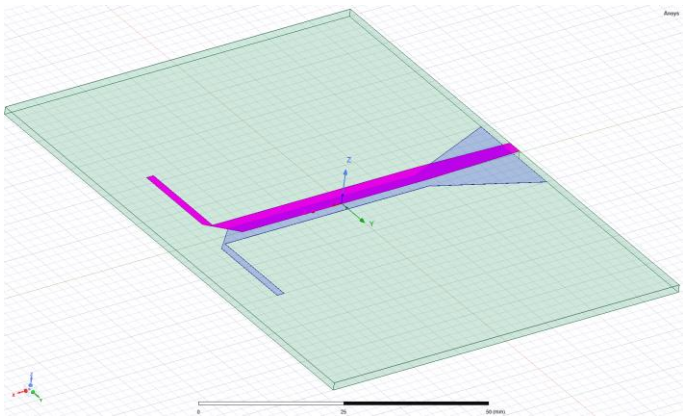
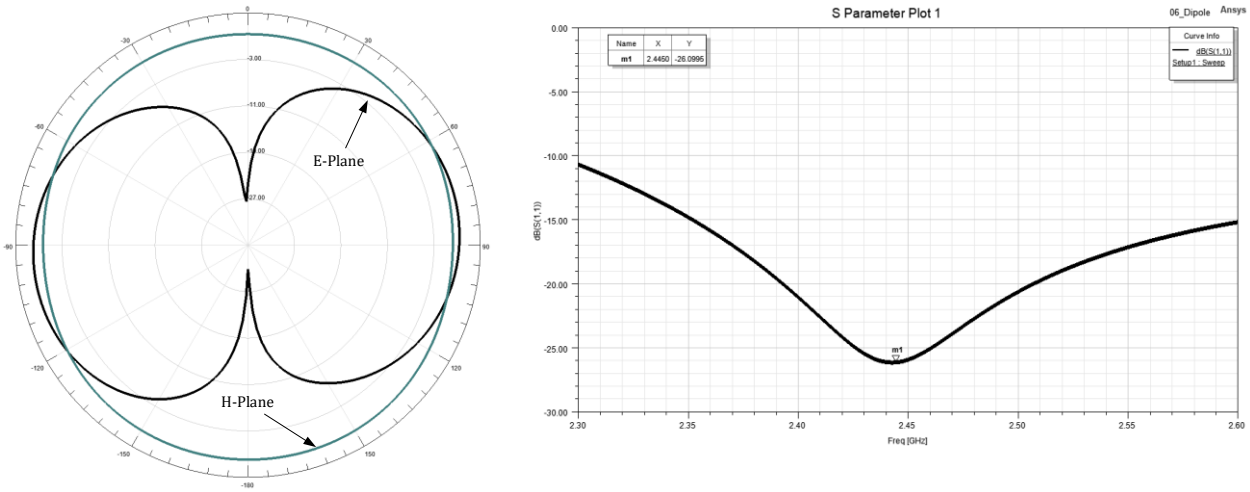


Fig. 2. Model of the antenna.

As a result of the optimization process, the following values were obtained for the antenna geometry L_{arm} = 20 mm; L_{feed} = 45 mm; L_{balun} = 20 mm; w_{arm} = 1.5 mm; w_{feed} = 4.1 mm; w_{balun} = 20 mm; w = 2.9 mm.

In Fig.3, the simulated results for the directivity diagram and the frequency responses of the antenna are shown. As it could be seen, the return loss is $RL = |S_{11}| \approx$ -21 dB at the operating band's left bound (f_L = 2.4 GHz), and $RL = |S_{11}| \approx$ -21.9 dB at the band's right bound (f_R = 2.483 GHz), and $RL = |S_{11}| \approx$ -

26.1 dB at the center frequency $f_0 = 2.442$ GHz. The gain of the antenna is $G \approx 2$ dBi. The polarization of the antenna is linear.



(a) (b)

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

The antenna designed in the course of the present research is small-sized and easily fabricated. VSWR value is less than 1.2 within the operating band 2.4…2.483 GHz. It can be noticed that the directivity pattern has some distortion relative to the pattern of an ideal dipole antenna. This is caused by the impact of the dielectric plate and feeding elements in the proximity of the radiating section of the antenna.

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. James J. R., Hall P. S., Wood C. Microstrip antenna: theory and design. – Iet, 1986.
4. Trubarov I.V. Design and Optimization of Two-Resonator Inset-Fed Printed Patch Antenna for 2.4 GHz Frequency Band // XV International Scientific Conference "Modern Challenges in Telecommunications" MCT-2021. Conference proceedings. Kyiv. Igor Sikorsky Kyiv Polytechnic Institute, 2021 – pp. 83 – 85. – ISSN(print)2663-502X.
5. Trubarov I.V. Design and Optimization of Coaxial-Fed Rectangular Two-Resonator Patch Antenna for 2.4 GHz Frequency Band // XV International Scientific Conference "Modern Challenges in Telecommunications" MCT-2021. Conference proceedings. Kyiv. Igor Sikorsky Kyiv Polytechnic Institute, 2021 – pp. 86 – 88. – ISSN(print)2663-502X.
6. Trubarov I.V. Design and Optimization of Two-Resonator Inset-Fed Printed Circular Patch Antenna for 2.4 GHz Frequency Band // XVI International Scientific Conference "Modern Challenges in Telecommunications" MCT-2022. Conference proceedings. Kyiv. Igor Sikorsky Kyiv Polytechnic Institute, 2022 – pp. 66 – 68. – ISSN(print)2663-502X.
7. Trubarov I.V. Design and Optimization of Coaxial-Fed Circular Two-Resonator Patch Antenna for 2.4 GHz Frequency Band // XVI International Scientific Conference "Modern Challenges in Telecommunications" MCT-2022. Conference proceedings. Kyiv. Igor Sikorsky Kyiv Polytechnic Institute, 2022 – pp. 69 – 71. – ISSN(print)2663-502X.

UDC 621.391.3

MICROSTRIP RING 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

МІКРОСМУЖКОВА КІЛЬЦЕВА АНТЕНА ДЛЯ ЧАСТОТНОГО ДІАПАЗОНУ 2,4 ГГЦ

Здійснено проєктування та оптимізацію несиметричної вібраторної антени із випромінювачем кільцевого типу для роботи у діапазоні 2,4 ГГц, виконаної за мікросмужковою технологією. Живлення антени здійснюється мікросмужковою лінією. Проведено моделювання роботи антени методом скінченних елементів в діапазоні робочих частот 2.4…2.483 ГГц. За результатами оптимізації антени забезпечено зменшення зворотних втрат, так що пристрій демонструє достатні для експлуатації характеристики у діапазоні частот, що значно перевищує робочу смугу. В межах робочої смуги частот КСХ розрахованої антени знаходиться в діапазоні 1…1.2.

Printed microstrip antennas are widely used in radiocommunication systems due to their small dimensions, low cost and possibility to be integrated at the common PCB with the device. There is a large number of small-size antenna types and design techniques that can be used for their analysis and fabrication [1] – [3]. Among the microstrip radiating structures, patch antennas are often used. However, these antennas are not omnidirectional and typically have gain of 6…9 dB [4 – 7]. To obtain omnidirectional directivity pattern, dipole or monopole antenna structures should be used.

In this paper, a microstrip monopole antenna for 2.4 GHz band is designed and simulated. The antenna is designed to operate in 2400…2483 MHz frequency band. As a radiating element, a ring topology was used. Antennas with such layout manifest ultrawideband operation. Therefore, even being optimized for 2.4 GHz band, the proposed antenna can be used in larger frequency range. The antenna can be used in mobile ISM band communication systems, such as Wi-Fi, Bluetooth or Zigbee applications. As numeric technique for the simulation, finite element method was used.

As a substrate for the antenna, FR4 laminate was used with the following parameters: dielectric constant ε_r = 4.4; thickness h = 1.5 mm; thickness of the top and bottom copper layers t = 0.018 mm; dissipation is defined by tan δ = 0.02.

The layout of the antenna is shown in Fig. 1. The antenna was designed so as to be fed by 50 Ω microstrip line or coaxial cable using SMA connector. The antenna of the selected type is ultrawideband and has pertinent performance in the frequency range that covers a few gigahertz higher 2 GHz frequency. As soon as it was designed primarily of 2.4 GHz band, its parameters were optimized to have the lowest return loss value in 2400…2483 GHz frequency range.

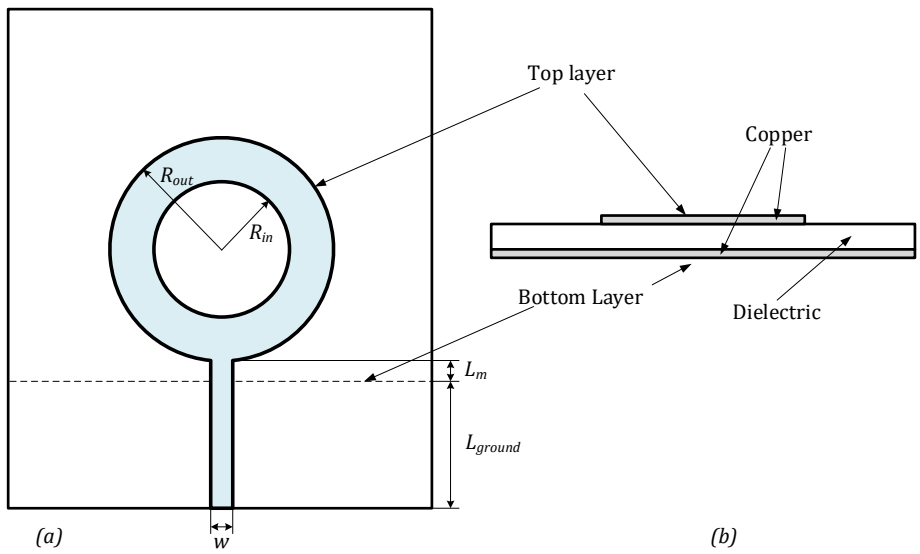
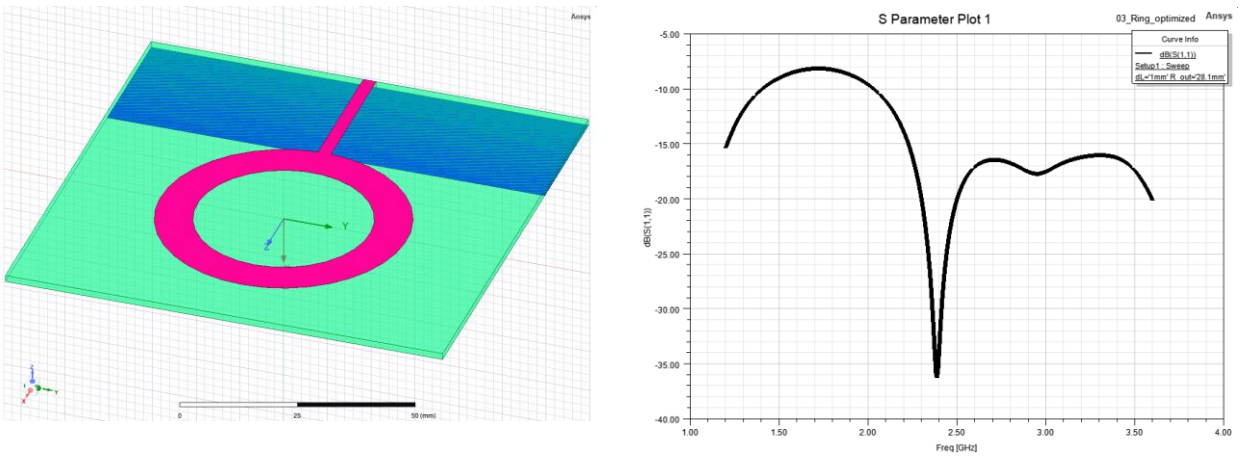


Fig.1. Dimensions of a microstrip dipole antenna. (a) Antenna dimensions. (b) Side view of the antenna.

The theory and design approach for the selected antenna type are considered in [1] – [3]. The design procedure contained the following stages: rough estimation of the geometry parameters according to general principles of the design of monopole antennas; analysis of the impact of L_m parameter on the antenna characteristics; optimization procedure over the two parameters: R_{in}, R_{out}.

As a result of the optimization process, the following values were obtained for the antenna geometry L_{ground} = 30 mm; L_m = 1 mm; w = 2.9 mm; R_{in} = 19.7 mm; R_{out} = 28.1 mm. The model of the antenna is shown in Fig. 2 (a), and Fig. 2 (b) shows the return loss of the antenna. It can be seen that the return loss is smaller than -20 dB in the operating band.

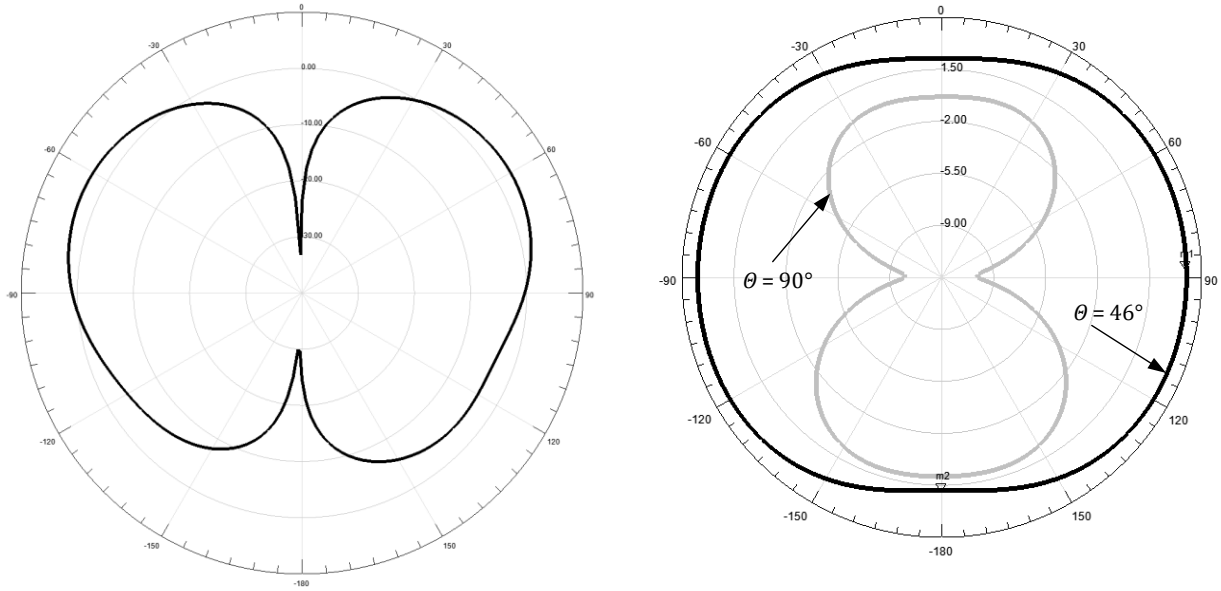


(a) (b)

Fig.2. (a) Model of the antenna. (b) Return loss of the antenna.

The antenna with a ring shape of monopole has semi-omnidirectional directivity pattern. The maximum radiation is observed not in the azimuthal plane, but is inclined for about 45 degrees. In Fig. 3, the radiation pattern of the antenna is presented. The observed gain is 2…4 dBi within the cone of the highest directivity,

which is observed for $\Theta = 46°$. The distortion of the radiation pattern is caused by the dielectric layer of PCB and the ring shape of the radiating element.



(a) (b)

Fig.3. Directivity pattern of the antenna. (a) E-plane. (b) H-plane.

The antenna designed in the course of the present research is small-sized and easily fabricated. VSWR value is less than 1.2 within the operating bandwidth 2.4…2.483 GHz. The antenna gain in the maximum of the main lobe is 2…4 dBi. The main lobe is inclined for about 45° relative to the azimuthal plane, which makes this solution well-suited for being mounted at considerable height for providing wide coverage area.

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. James J. R., Hall P. S., Wood C. Microstrip antenna: theory and design. – Iet, 1986.
4. Trubarov I.V. Design and Optimization of Two-Resonator Inset-Fed Printed Patch Antenna for 2.4 GHz Frequency Band // XV International Scientific Conference "Modern Challenges in Telecommunications" MCT-2021. Conference proceedings. Kyiv. Igor Sikorsky Kyiv Polytechnic Institute, 2021 – pp. 83 – 85. – ISSN(print)2663-502X.
5. Trubarov I.V. Design and Optimization of Coaxial-Fed Rectangular Two-Resonator Patch Antenna for 2.4 GHz Frequency Band // XV International Scientific Conference "Modern Challenges in Telecommunications" MCT-2021. Conference proceedings. Kyiv. Igor Sikorsky Kyiv Polytechnic Institute, 2021 – pp. 86 – 88. – ISSN(print)2663-502X.
6. Trubarov I.V. Design and Optimization of Two-Resonator Inset-Fed Printed Circular Patch Antenna for 2.4 GHz Frequency Band // XVI International Scientific Conference "Modern Challenges in Telecommunications" MCT-2022. Conference proceedings. Kyiv. Igor Sikorsky Kyiv Polytechnic Institute, 2022 – pp. 66 – 68. – ISSN(print)2663-502X
7. Trubarov I.V. Design and Optimization of Coaxial-Fed Circular Two-Resonator Patch Antenna for 2.4 GHz Frequency Band // XVI International Scientific Conference "Modern Challenges in Telecommunications" MCT-2022. Conference proceedings. Kyiv. Igor Sikorsky Kyiv Polytechnic Institute, 2022 – pp. 69 – 71. – ISSN(print)2663-502X.

УДК 621.391

МОДЕЛЮВАННЯ МЕРЕЖІ SDN З ВИКОРИСТАННЯМ ВІДКРИТОЇ МЕРЕЖЕВОЇ ОПЕРАЦІЙНОЇ СИСТЕМИ ONOS

Романов О.І., Сколець С.С., Марінов А.І.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: a_i_romanov@ukr.net, serskols@gmail.com, anton_marinov@ukr.net

SDN NETWORK SIMULATION USING ONOS OPEN NETWORK OPERATING SYSTEM

This article demonstrates how to modify the parameters of network components and communication channels while describing network topology, as well as test the capabilities of a network that is subordinated to ONOS controller with specified network parameters, such as bandwidth and maximum queue-size.

У роботі досліджені параметри пропускної здібності мережі SDN, на базі використання програмних продуктів Mininet та ONOS, які є у відкритому доступі. Показано як змінювати параметри мережевих компонентів та каналів зв'язку при описі топології мережі. Проаналізовано вплив різних протоколів та розмір черги на пропускну здібність мережі.

Оскільки Mininet являється загальною платформою-емулятором, то при запуску мережі без зазначення мережевих параметрів вона не відповідає дійсній SDN мережі. Тому з початку потрібно зазначити низку параметрів і провести декілька кроків налаштування, щоб мережа відповідала вимогам реальної SDN мережі[1].

В нашому випадку буде використовуватись топологія мережі (рис. 1), яка написана на вищому рівні Mininet API (Python API). Топологія Mininet описана в окремому файлі розширення "`.py`" з залученням сторонніх бібліотек для більш гнучких налаштувань мережі. В роботі була використана бібліотека TCLink, яка надає змогу задавати пропускну здібність, затримку, джиттер у каналах зв'язку, а також RemoteController для описання ONOS контролера, якій в подальшому буде підключений до мережі в якості централізованого органу управління[2][6].

Конфігураційний файл мережі/топології має наступний вигляд:

```
#!/usr/bin/python
## імпорт бібліотек python
from mininet.topo import Topo
from mininet.net import Mininet
from mininet.link import TCLink
from mininet.node import Controller, OVSSwitch, RemoteController
from mininet.cli import CLI
from mininet.log import setLogLevel

def multiControllerNet():
    ##  додання мережевих елементів
    net = Mininet( controller=RemoteController, switch=OVSSwitch, link=TCLink )
    c1 = RemoteController( 'c1', ip='172.17.0.6', port=6653 )
    s10 = net.addSwitch( 's10', dpid='0000000000000010', mac='00:00:00:00:SW:10' )
    ...
    h11 = net.addHost( 'h11', ip='10.0.0.11/24', mac='00:00:00:00:0H:11' )
    ...

    ## додання мережевих зв'язків
    net.addLink( s10, s20, bw=100)
    ...

    ## запуск мережевих компонентів
    net.start()
    c1.start()
    s10.start( [ c1 ] )
    ...
    CLI( net )
if __name__ == '__main__':
    setLogLevel( 'info' )  # for CLI output
    multiControllerNet()
```

Зазначений код описує процес запуску основних елементів мережі. Цей процес складається з наступних етапів:

- імпорт бібліотек python, що надають змогу компілятору python розуміти синтаксис опису саме топології Mininet;
- додання мережевих елементів: комутаторів з підтримкою OpenFlow, хостів, а також задання їм унікальні адреси та ідентифікатори в мережі, описання розташування контролеру та порт на якому він приймає включення;
- додання мережевих зв'язків - підключення комутаторів між собою, а також підключення хостів до комутаторів;
- запуск мережевих компонентів, Mininet консолі, а також підключення кожного комутатора до контролера ONOS.

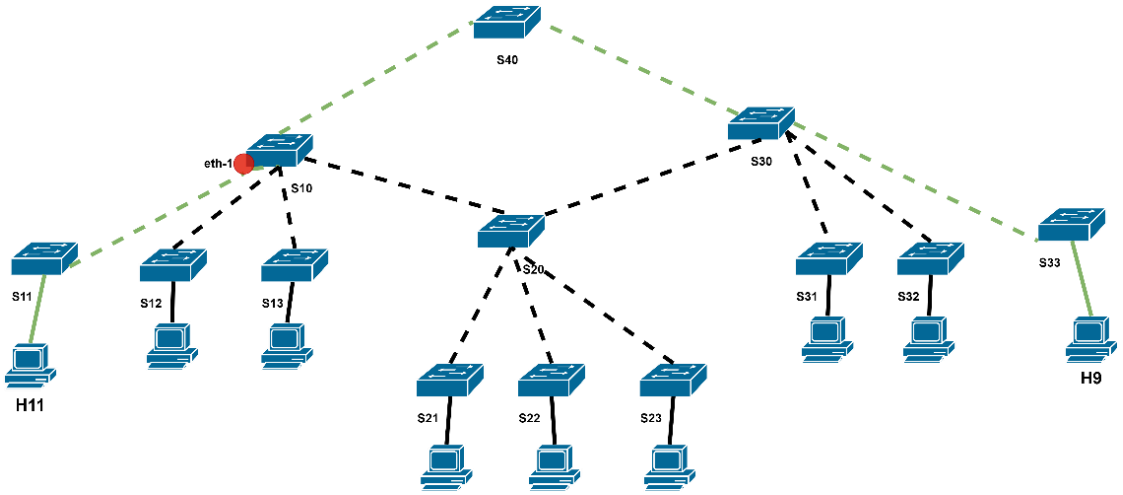


Рис.1. Топологія SDN мережі.

Після запуску мережі необхідно провести тестування параметрів функціонування мережі. В роботі проведено тестування пропускної здатності каналів зв'язку у напрямку від h11 до h9. Для цього, організована передача UDP трафіку при різному навантаженні каналів зв'язку і при різній швидкості передачі. При цьому були використані наступні вихідні данні:

- топологія мережі, що зображена на рис.1;
- інформаційний напрямок зв'язку між хостами h11 - h9;
- кількість проміжних вузлів(комутаторів) – 3;
- навантаження в пакетах, що передається – 500 Мбайт;
- швидкість передачі у лініях зв'язку – 100 Мбіт/с.

У ході проведення досліду було знято часові діаграми швидкості передачі UPD трафіку. Крок підвищення навантаження у лініях зв'язку становить: 10%, 50%, 100% від максимально заданої швидкості передачі лінії зв'язку. Тобто 10, 50, 100Мбіт/с, відповідно. Часові діаграми наведені на рис. 2.

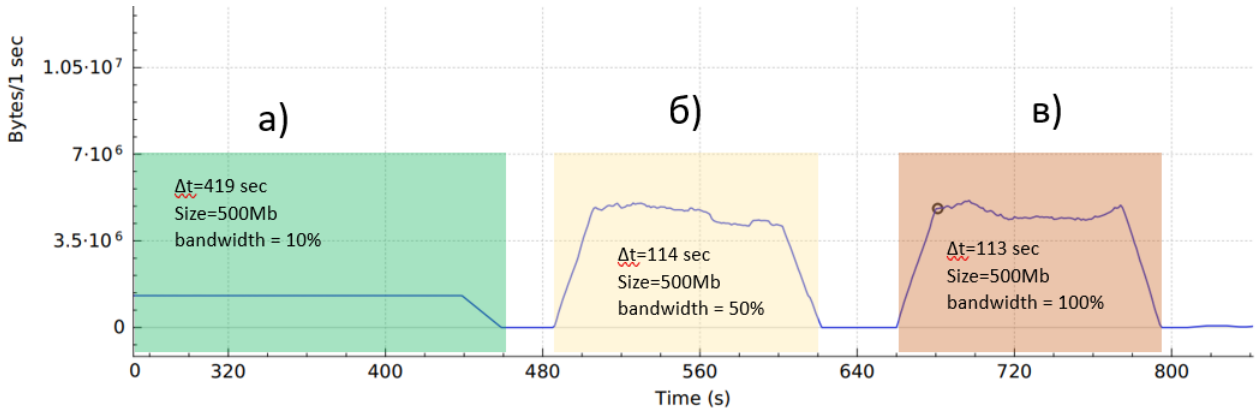


Рис. 2. Швидкість передачі трафіку каналом зв'язку при: а) навантаження 10%; б) навантаження 50%; в) навантаження 100%.

Наступним етапом тестування мережі стала перевірка характеру поведінки мережі шляхом зняття показників функціонування при зміні показника максимального буферу пакетів в черзі (queue size). Відповідне дослідження дало змогу перевірити особливості передачі TCP/UDP трафіку.

Зміна довжини буферу пакетів проводилась на всіх інтерфейсах в напрямку передачі трафіку наступним чином: 1, 5, 10, 25, 50, 75, 100, 200, 500 пакетів.

Результати поведінки мережі відображено на рис. 3

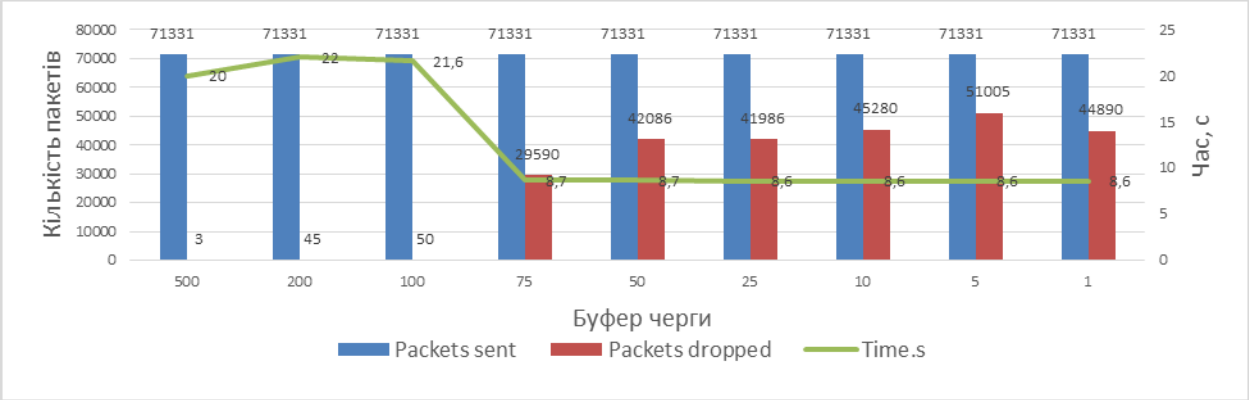


Рис. 3а. Параметри трафіку при передачі за протоколом UDP.

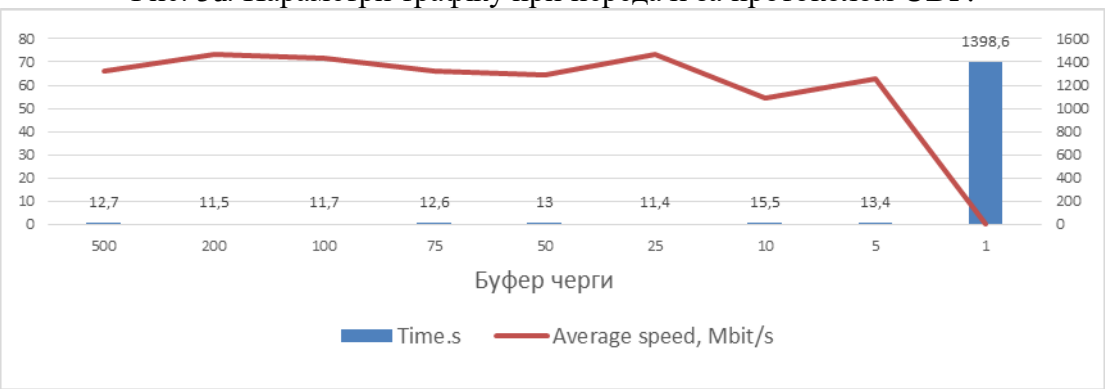


Рис. 3б. Параметри трафіку при передачі за протоколом TCP.

Проведені дослідження дозволяють визначити де які особливості. Побудова мережі SDN довільної топології вимагає додаткового написання програмного коду на мові python. Це дає можливість створювати необхідні зв'язки як між елементами мережі, так і між елементами керування мережею.

В роботі, використовуючи побудовану топологію та перераховані вихідні дані, було знято часові діаграми при навантаженні напрямку зв'язку. Відображені результати показали, що при навантаженні лінії зв'язку до 50%, передача відбувається з постійною швидкістю без суттєвих змін, що не можна сказати при навантаженні більше 50%. В такому випадку, характер швидкості непередбачуваний, хоча в обох випадках, переданий об'єм трафіку доставляється без втрат[4].

Проводячи аналіз досліду, при зміні queue-size, можна зробити висновки:

При передачі UDP трафіку, встановивши значення max_queue_size – 100 пакетів і більше, втрати майже непомітні (досягають 0,07% максимум), однак при зменшенні буферу черги від 1 до 100 пакетів, втрати можуть бути суттєвими, тобто 72-41%.

При передачі TCP трафіку, втрати не спостерігаються, хоча швидкість передачі даних зменшується відповідно до зменшення параметру буфера (max_queue_size). Це пояснюється головною особливістю TCP трафіку, а саме наявністю підтверджень (ACK) від отримувача, які повідомляють відправника про успішну доставку кожного пакету[3][5]. Якщо відправник не отримує підтвердження вчасно, він повторно надсилає пакет до отримувача. У UDP така гарантія відсутня, тому пакети можуть бути втрачені в разі перевантаження мережі або інших проблем з передачею даних.

Треба відмітити суттєвий недолік проведених досліджень на базі цих програмних продуктів. При моделюванні ми не змогли зробити балансування трафіку. Тому коли з'являється перевантаження в напрямку зв'язку і при цьому є наявний вільний ресурс в мережі, контролер ONOS не реагує на перевантаження і не змінює шляхи передавання трафіку. Це говорить о том, що ця функція чи поки що відсутня у цьому програмному продукті, чи ми не змогли її підключити.

Література

1. Документація ONOS: https://wiki.onosproject.org/display/ONOS/Documentation
2. S. Rathee, S. Rathee, K. Haribabu. GlobeSnap: An Efficient Globally Consistent Statistics Collection for Software-Defined Networks/Journal of Network and Systems Management 2021, 29(3)/DOI:10.1007/s10922-021-09601-z
3. Romanov, O., Nesterenko, M., Mankivskyi, V., Zhuk, O. Principles of Building Modular Control Plane in Software-Defined Network//Lecture Notes in Networks and Systems, 2023, 548, pp. 333–355, DOI: 10.1007/978-3-031-16368-5_17
https://link.springer.com/chapter/10.1007/978-3-031-16368-5_17
4. Romanov, O., Korniienko N., Svyd I., Romanov A. Optical Network Management by ONOS-Based SDN Controller, September 2022, Radiotekhnika, DOI:10.30837/rt.2022.3.210.16
5. Pedro Sousa, Gonçalo Pereira, Jose Silva. Comparative Study of Software-Defined Networking (SDN) Traffic Controllers, Jun 2019, 2019 14th Iberian Conference on Information Systems and Technologies (CISTI),DOI: 10.23919/CISTI.2019.8760997
6. Romanov, O., TT Dong., Nesterenko, M. The possibilities for deployment eco-friendly indoor wireless networks based on LiFi technology/(2020) Proceedings of International Conference on Applied Innovation in IT, 8 (1), pp. 41-48.

УДК 621.382

ІНТЕГРАЦІЯ АРХІТЕКТУРИ IMS В МЕРЕЖІ 5G

Верес Л.А.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: veresleonid@gmail.com

INTEGRATION OF THE IMS ARCHITECTURE IN THE 5G NETWORK

With the advent of the 5G network, the Internet of Things (IoT) and the increased use of mobile devices, mobile operators are forced to improve the quality of their networks and ensure a stable connection of users to the Internet and other services. In this regard, the integration of the IMS (IP Multimedia Subsystem) architecture in the 5G network is becoming more and more relevant.

IMS is a standard architecture that provides the ability to transmit voice information and services using IP protocols. IMS provides a connection to the world of the Internet and the traditional telephony network. The integration of IMS into the 5G network ensures excellent quality of services and improves the efficiency of using network resources.

З появою мережі 5G, інтернет речей (IoT) та розширеного використання мобільних пристроїв, мобільні оператори вимушені підвищувати якість своїх мереж та забезпечувати стабільне підключення користувачів до інтернету та інших послуг. У зв'язку з цим, інтеграція архітектури IMS (IP Multimedia Subsystem) в мережі 5G стає дедалі більш актуальною.
IMS - це стандартна архітектура, яка забезпечує можливість передачі голосової інформації та послуг з використанням IP-протоколів. IMS забезпечує з'єднання зі світом інтернету та традиційної мережі телефонії. Інтеграція IMS в мережу 5G забезпечує відмінну якість послуг та забезпечує підвищення ефективності використання ресурсів мережі. Взаємодія архітектури IMS та мережі 5G буде мати такий вигляд (Рис. 1). Однак, як і з будь-яким технологічним рішенням, інтеграція архітектури IMS в мережу 5G має свої переваги та недоліки.

Переваги інтеграції IMS в мережу 5G:

1. Покращення якості послуг: Інтеграція IMS в мережу 5G забезпечує передачу голосової інформації з використанням IP-протоколів. Це дозволяє забезпечувати відмінну якість послуг та підвищувати задоволеність користувачів.

2. Використання ресурсів мережі: Інтеграція IMS дозволяє мобільним операторам використовувати ресурси мережі більш ефективно. Це може бути досягнуто за рахунок використання одного протоколу для передачі голосу та інших даних.

3. Забезпечення більш швидкого доступу до послуг: IMS дозволяє мобільним операторам забезпечувати більш швидкий доступ до послуг для

користувача

4. Забезпечення більшої безпеки: Інтеграція IMS дозволяє мобільним операторам забезпечувати більшу безпеку та захист від атак. IMS використовує шифрування даних, що забезпечує безпеку передачі інформації.

5. Підвищення ефективності мережі: Інтеграція IMS дозволяє мобільним операторам підвищувати ефективність мережі шляхом зменшення простою мережі та збільшення її пропускної здатності.

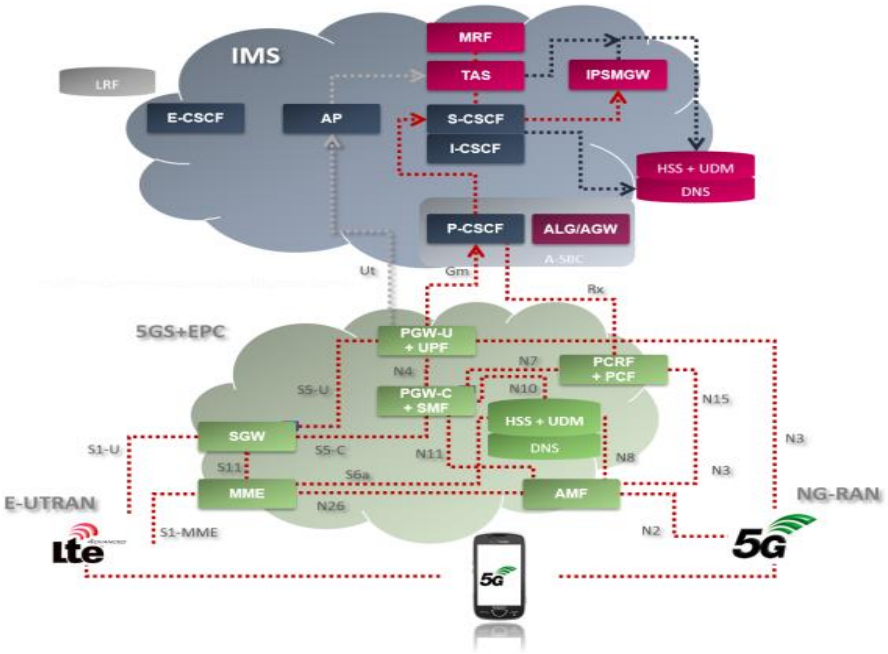


Рис. 1. Побудова мережі 5G на базі IMS.

Недоліки інтеграції IMS в мережу 5G:

1. Високі витрати на впровадження: Інтеграція IMS в мережу 5G вимагає великих витрат на впровадження нової архітектури та протоколів.

2. Складність впровадження: Інтеграція IMS в мережу 5G потребує значної технічної експертизи, а також навчання персоналу для роботи з новими протоколами та інтерфейсами.

3. Проблеми зі сумісністю: Інтеграція IMS в мережу 5G може виникнути проблеми зі сумісністю зі старішими версіями мереж та пристроїв.

Інтеграція архітектури IMS в мережу 5G - складний технологічний процес, що потребує розробки та реалізації певних протоколів та інтерфейсів. Для того, щоб забезпечити взаємодію мережі 5G з архітектурою IMS, виділимо основні з них:

SIP (Session Initiation Protocol): Протокол SIP використовується для ініціювання та управління сеансами зв'язку, такими як голосові та відеозв'язки.

RTP (Real-Time Transport Protocol): RTP використовується для передачі голосових та відеоданих в реальному часі.

Diameter: Diameter - це протокол управління сеансами, який використовується для авторизації та аутентифікації користувачів, а також для

управління сеансами.

IMS Interworking Function (IWF): IWF - це інтерфейс, який забезпечує інтероперабельність між IMS та іншими мережами.

IMS Centralized Services (ICS): ICS - це інтерфейс, який забезпечує централізовані сервіси, такі як пересилання повідомлень, групові дзвінки та конференції.

IMS Media Plane (IMSP): IMSP - це інтерфейс, який забезпечує передачу голосових та відеоданих між IMS та іншими мережами.

IP Multimedia Subsystem Application Programming Interface (IMS API): IMS API - це інтерфейс програмного забезпечення, який дозволяє розробникам створювати нові додатки, що працюють в IMS.

IP Multimedia Subsystem Service Control Function (IMS SCF): IMS SCF - це інтерфейс, який забезпечує управління сервісами IMS.

Висновки. Інтеграція архітектури IMS в мережу 5G має багато переваг для мобільних операторів та користувачів мережі. Це дозволяє операторам забезпечувати нові послуги та покращувати якість зв'язку, а також забезпечувати більшу безпеку та захист від атак. Однак, впровадження нової архітектури та протоколів потребує значних витрат та технічної експертизи. На щастя, існує широкий спектр протоколів та інтерфейсів, необхідних для успішної інтеграції IMS в мережу 5G. Знання цих протоколів та інтерфейсів може допомогти мобільним операторам успішно впроваджувати IMS в мережу 5G та забезпечити більшу якість зв'язку та підвищення ефективності мережі.

Література

1. Скулиш М.А., Романов О.І., Глоба Л.С. Принцип обслуговування потоків у гетерогенному телекомунікаційному середовищі //Скулиш М.А., Романов О.І., Глоба Л.С. //Записки університету ім. В.І. Вернадського, - Том 29 (68) № 2 – 2018 –С. 92-98.
2. O.I. Romanov, M.M. Nesterenko, L.A. Veres. IMS: Model and calculation method of telecommunication network's capacity // Proceedings of the 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo) 11-15 Sept. 2017 Year, Odessa, Ukraine. - IEEE Conference Publications (IEEE Xplore Digital Library, DOI: 10.1109/UkrMiCo.2017.8095412), 2017. – P. 1-4.
3. Mariia Skulysh, Romanov Oleksandr. The structure of a mobile provider network with network functions virtualization. // Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), 2018 14th International Conference on. IEEE, 2018 - Pages: 1032 - 1034 DOI: 10.1109/TCSET.2018.8336370.
4. VoIMS – IMS and 5G - https://realtimecommunication.wordpress.com/2017/10/31/ims-and-5g/
5. 5G Implementation Guidelines / July 2019 - https://www.gsma.com/futurenetworks/wp-content/uploads/2019/03/5G-Implementation-Guideline-v2.0-July-2019.pdf.

УДК 621.395

ДОДАТКОВИЙ МЕХАНІЗМ МЕРЕЖЕВОЇ ВЗАЄМОДІЇ IN KUBERNETES

[1]**Маньківський В.Б.**, [2]**Конахович Г.Ф.**, [2]**Романов А.О.**
[1]*Навчально-науковий інститут телекомунікаційних систем*
КПІ ім. Ігоря Сікорського, Україна
[2]*Національний авіаційній університет, Київ, Україна*
E-mail: tks@nau.edu.ua; v.b.mankivskiy@gmail.com; anton3329@gmail.com

ADDITIONAL NETWORK INTERCONNECTION IN KUBERNETES

Containerization of applications and their deployment in a cloud environment is a key factor in ensuring the scalability, elasticity and availability of network applications. Kubernetes, a state-of-the-art container management platform, provides many capabilities for automatically scaling resources to ensure high availability and application performance. However, there are limitations that lead to the need to improve the mechanisms of network interaction, especially in conditions of uncertainty and variability of the environment.

Контейнеризація програм і їх розгортання в хмарному середовищі є ключовим фактором забезпечення масштабованості, еластичності та доступності мережевих програм. Kubernetes, найсучасніша платформа керування контейнерами, надає багато можливостей для автоматичного масштабування ресурсів для забезпечення високої доступності та ефективності програм. Однак існують обмеження, які призводять до необхідності вдосконалення механізмів мережевої взаємодії, особливо в умовах невизначеності та мінливості середовища.

Мережа є критично важливим компонентом будь-якої розподіленої системи, включно з Kubernetes. Однак проблеми з мережею можуть вплинути на доступність, надійність і продуктивність програм, розгорнутих у Kubernetes. У цій роботі ми досліджуємо вплив мережевих проблем у Kubernetes і аналізуємо найкращі методи виявлення та вирішення цих проблем.

Kubernetes - це популярна платформа оркестровки контейнерів з відкритим вихідним кодом, яка дає змогу організаціям масштабно розгортати та керувати контейнерними програмами. Однією з ключових переваг Kubernetes є його здатність абстрагуватися від основної інфраструктури, що полегшує розробникам зосередження на створенні та розгортанні своїх програм. Проте мережа є критично важливим компонентом будь-якої розподіленої системи, включаючи Kubernetes, і проблеми з мережею можуть вплинути на доступність, надійність і продуктивність програм, розгорнутих на Kubernetes.

Вплив мережевих проблем. Проблеми з мережею в Kubernetes можуть проявлятися різними способами, включаючи проблеми з підключенням, проблеми з вирішенням DNS, збої балансувальника навантаження тощо. Ці проблеми можуть спричинити простій програми, повільний час відгуку та

інші проблеми, які можуть негативно вплинути на роботу кінцевого користувача. Наприклад, якщо контейнер не може підключитися до бази даних через проблему з мережею, програма може вийти з ладу або перестати відповідати, що призведе до простою для кінцевих користувачів.

Виявлення мережевих проблем. Щоб виявити проблеми з мережею в Kubernetes, важливо відстежувати мережевий трафік між контейнерами та вузлами, а також справність мережевих компонентів, таких як DNS і балансувальників навантаження. Kubernetes надає кілька вбудованих інструментів для моніторингу мережі, зокрема сервер Kubernetes API, kube-proxy і core_dns. Крім того, сторонні інструменти моніторингу, такі як Prometheus і Grafana, можна використовувати для моніторингу продуктивності мережі та виявлення проблем.

Вирішення проблем мережі. Вирішення мережевих проблем у Kubernetes може бути складним завданням, оскільки є багато потенційних причин і конфігурацій, які слід враховувати. В роботі ми розглянули одну з найкращих практик [2,3] з точки зору спорідненої технології, які можуть допомогти швидко виявити та вирішити проблеми з мережею. До неї належить використання сервісної мережі Istio, щоб керувати трафіком між контейнерами та вузлами.

Istio - це популярна сітка сервісу з відкритим кодом, яка надає комплексне рішення для керування трафіком між контейнерами та вузлами в Kubernetes. Istio використовує модель sidecar, де проксі (Envoy) розгортається поряд з кожним контейнером у модулі. Цей проксі-сервер перехоплює весь мережевий трафік до та з контейнера та дозволяє Istio керувати трафіком між контейнерами та вузлами.

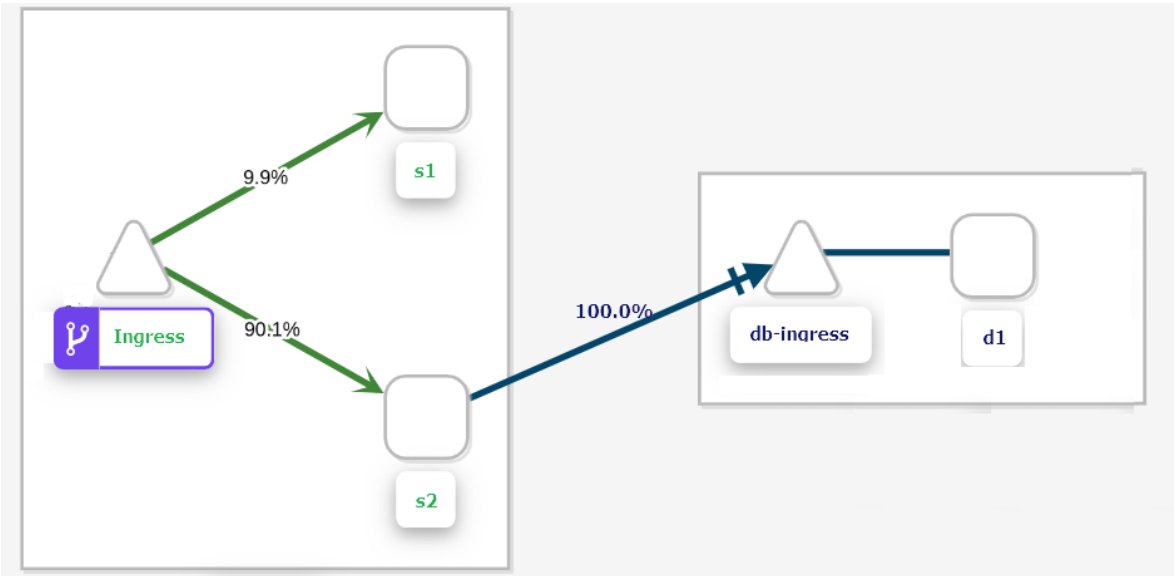


Рис. 1. Istio routing.

Визначені правила маршрутизації достатньо прості для зміщення акценту на реалізацію (Рис. 1): після розгортання сервісів Istio (sidecar service) можна визначити правила маршрутизації за допомогою функцій керування трафіком Istio. Це дає змогу контролювати, як трафік проходить між контейнерами та вузлами у вашому кластері Kubernetes. Наприклад, можна визначити правила, по яким маршрутизується трафік на основі конкретних заголовків, шляхів або агентів користувачів.

Рекомендації. Відстежуйте та захищайте трафік: Istio також надає функції моніторингу та безпеки, які дозволяють відстежувати мережевий трафік і захищати ваші програми Kubernetes. Ви можете використовувати Istio для застосування таких політик, як обмеження швидкості, контроль доступу та шифрування.

Масштабуйте Istio та керуйте ним. Нарешті, ви можете масштабувати Istio та керувати ним за допомогою таких інструментів Kubernetes, як kubectl і Helm. Ви можете використовувати ці інструменти для розгортання нових конфігурацій Istio, оновлення існуючих конфігурацій і керування такими компонентами Istio, як площина керування та площина даних.

Загалом, Istio надає потужне та гнучке рішення для керування трафіком між контейнерами та вузлами в Kubernetes. Використовуючи Istio, ви можете переконатися, що ваші програми Kubernetes надійні, продуктивні та безпечні.

Висновок. Мережа є критично важливим компонентом будь-якої розподіленої системи, включно з Kubernetes. Проблеми з мережею можуть вплинути на доступність, надійність і продуктивність програм, розгорнутих у Kubernetes. Тому важливо швидко виявляти та вирішувати ці проблеми, використовуючи передові практики, такі як моніторинг мережевого трафіку, використання сітки служби та обмеження трафіку за допомогою мережевих політик. Дотримуючись цих найкращих практик, організації можуть переконатися, що їхні програми надійні та продуктивні, навіть якщо виникають проблеми з мережею.

Література

1. Xie, Z., Yuan, X., Wang, J., Ju, S. “Encoder-Decoder Network with Cross-Match Mechanism for Answer Selection” In: Sun, Chinese Computational Linguistics. CCL 2019. Lecture Notes in Computer Science(), vol 11856. Springer, Cham. https://doi.org/10.1007/978-3-030-32381-3_6
2. Romanov O, Mankivskyi V. Optimal traffic distribution based on the sectoral model of loading network elements, IEEE Problems of Infocommunications. Science and Technology Trans. Multimedia, 2019, pp. 210–219.
3. Mankivskyi Volodymyr and Pedko Andryi Concept of edge computing in mobile operator network // Modern challenges in telecommunications, vol. 14, 2020, pp. 51–54.
4. M. Xiao et al., Millimeter Wave Communications for Future Mobile Networks // IEEE JSAC, vol. 35, no. 9, Sept. 2017, pp.1909–35.
5. Oleksandr I Romanov, Mykola M Nesterenko, Nadiia O Fesokha and Volodymyr B Mankivskyi. Evaluation of productivity virtualization technologies of switching equipment telecommunications networks. // National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, 2020 - pp.: 132 – 138

УДК 681.2+681.5

НАМОТОЧНА МАШИНА ДЛЯ ВИГОТОВЛЕННЯ КОТУШОК ВОЛОКОННО-ОПТИЧНИХ ГІРОСКОПІВ

Іванов С.В., Олійник П.Б., Вірченко Г.А.
НДІ телекомунікацій КПІ ім. Ігоря Сікорського, Україна
E-mail: ivanov.sergiy@lll.kpi.ua

Winding machine for manufacturing of fiber-optic gyro coils

Winding machine for manufacturing of fiber-optic gyro coils is presented. Structure of the machine hardware part and its software is shown, and main functions of the machine are described.

Для вимірювання кутової швидкості широко використовують волоконно-оптичні гіроскопи (ВОГ). Практичне застосування такі прилади знайшли у телекомунікації в системах орієнтації та стабілізації антен, зокрема супутникового зв'язку, в системах орієнтації та навігації космічних апаратів, пілотованої авіації та безпілотних апаратів – авіаційних, надводних, підводних.

Створення данного класу приладів стало можливим лише з розвитком і вдосконаленням елементної бази квантової електроники. Принцип дії оптичних гіроскопів заснований на вихровому ефекті Саньяка. Ключовим елементом такого приладу є котушка, намотана з оптичного волокна. Від якості її намотки залежить точність приладу та стабільність його параметрів. Оскільки процес намотки котушки трудомісткий, то для його автоматизації проектують намоточні машини.

Перші дослідження в галузі створення намоточних машин розпочато ще в 1990-х. Наприклад, в [1] подано загальні настанови з проектування такої машини. У 2001 році автори [2] представили машину з системою підтримання сталого натягу волокна, автоматичним перемиканням подачі волокна з робочих котушок. Це необхідно для котушок зі складною намоткою, наприклад квадрупольною, та контролю дефектів намотки у процесі роботи машини. Аналогічний підхід застосовано в роботі [3].

У [4] запропонано намоточну машину на основі складної системи, заснованої на розподілених мережевих технологіях і з застосуванням нечіткої логіки. Такий підхід знімає проблеми, пов'язані з обмеженною обчислювальною потужністю керуючих пристроїв. Водночас він знижує оперативність керування машиною, що може призвести до виникнення додаткових дефектів.

Автори [5] та [6] створили намоточну машину, в якій застосовано інший принцип. Усе керування та обробку даних зосереджено на одному головному комп'ютері (використано технологію віртуальних пристроїв LabView). Недоліком такого підходу є необхідність застосування потужного промислового комп'ютера та дорогого програмного забезпечення. При цьому основні принципи керування - підтримання сталого натягу волокна, автоматичне перемикання подачі волокна, контроль якості намотки – незмінні у всіх розробках. Створена машина орієнтована на виготовлення котушок з квадрупольною намоткою.

У даній публікації представлено розроблювану в НДІ ТК КПІ ім. Ігоря Сікорського намоточну машину (державний реєстраційний номер 0122U200937). Для досягнення високої стабільності роботи гіроскопа в мінливих умовах навколишнього середовища, зокрема з урахуванням чутливості вихідного сигналу до температури, намоточна машина забезпучує виготовлення котушок з кількома типами намоток таких як квадрупольною, модифікованою квадрупольною та іншими [7]. Схему машини для намотки оптичного волокна, засновану на досвіді побудови таких машин іншими дослідниками [1,2, 5, 6], наведено на рис. 1.

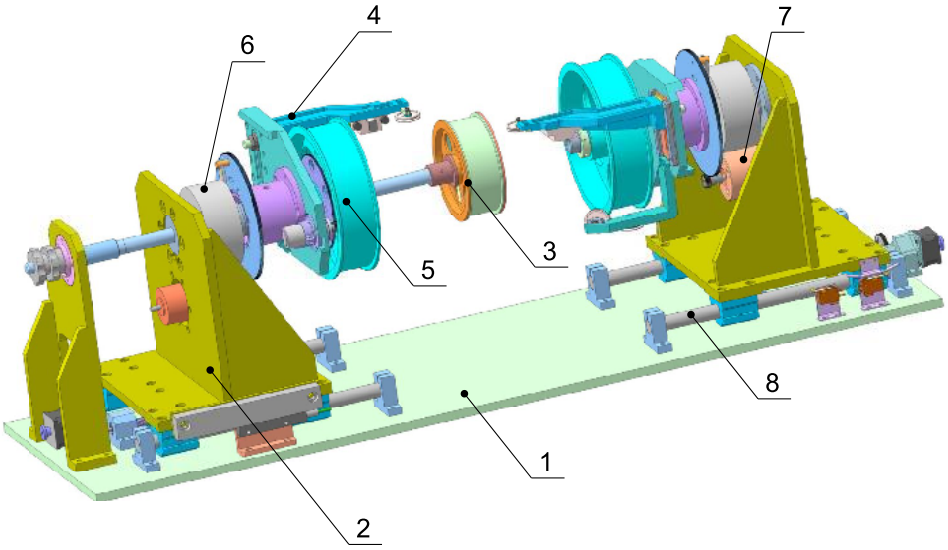


Рис. 1. Машина для намотки оптичного волокна: 1 – основа, 2 – намотувальний модуль, 3 – котушка ВОГ, 4 – водило, 5 – робоча котушка, 6 – вузол кріплення осі водила, 7 – редуктор, 8 – лінійні направляючі

Для намотки волокна на котушку ВОГ застосовуються два намоточних модулі 2 з водилами 4. За рахунок керування рухом цих модулів з використанням лінійних направляючих та водил забезпечується рівномірна укладка волокна на котушку ВОГ 3 та стабілізація його натягу при намотці.

Використання системи машинного зору забезпечує виявлення дефектів (візуально й напівавтоматично), оцінку й класифікацію за типами дефектів, ведення статистики, а також збереження та видачу результатів роботи за заданий період із можливістю автоматичного створення звітів. Правильна класифікація виявлених дефектів дозволяє визначити причини їх виникнення, своєчасно внести необхідні коригування у виробничий процес. Оптична камера, що входить до системи машинного зору на рис.1 не показана.

Для керування машиною, на відміну відіснуючих аналогів, запропоновано застосувати комбінований підхід, а саме: для безпосереднього керування процесом намотки, включаючи позиціонування намоточних модулів та стабілізація натягу волокна використовується спеціально розроблений електронний блок керування, а для загального керування процесом намотки (як пульт керування) та виявлення дефектів застосовуватиметься персональний комп'ютер. Це дозволить суттєво здешевити апаратну частину машини.

Програмне забезпечення (ПЗ) машини складається відповідно з ПЗ електронного блока керування та ПЗ верхнього рівня.

ПЗ електронного блока керування призначене для керування машиною на низькому рівні, забезпечуватиме підтримання заданого натягу волокна, рівномірність укладки волокна на котушки, а також виконання намотки волокна згідно з програмою намотки, заданої з пульта керування.

ПЗ верхнього рівня (рис. 2) буде встановлено на пульті керування, забезпечуватиме загальне керування намоткою, включаючи керування режимом намотки, задання натягу волокна та контроль дефектів намотки в реальному часі.

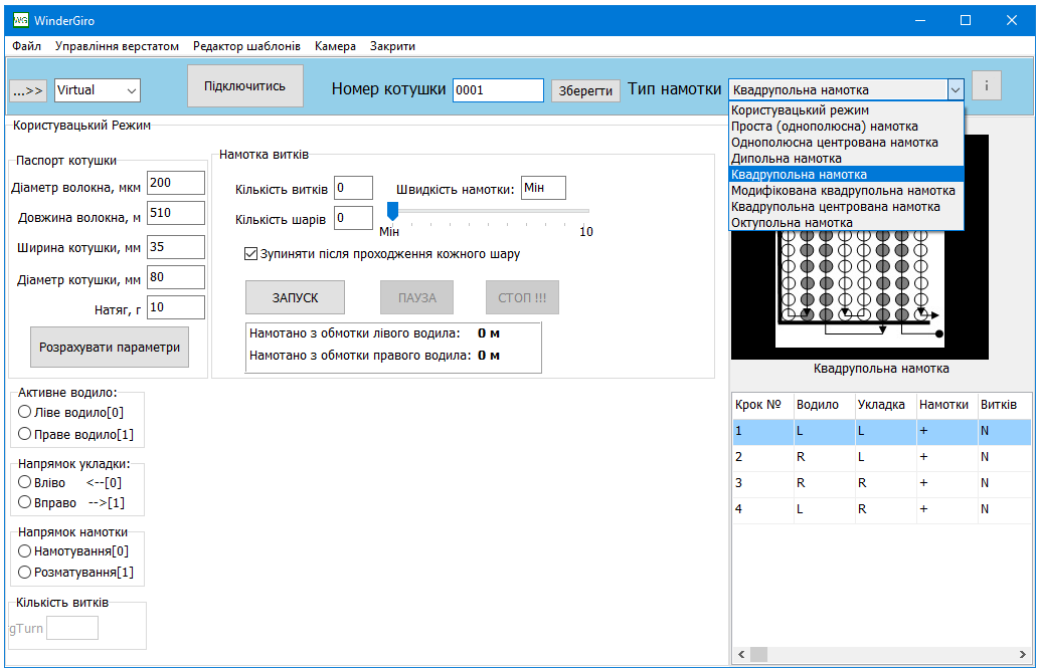


Рис. 2. Інтерфейс ПЗ верхнього рівня

На даний момент дослідний зразок намоточної машини знаходиться у процесі виготовлення. Результати розробки буде представлено після випробувань у технічній звітності по науково-дослідній роботі, на міжнародних комунікативних форумах, всеукраїнських та регіональних науково-технічних/промислових виставкових заходах, а також у наукових журналах.

Література

1. De Fazio, Thomas L. Development issues for automating quadrupole-pattern optical-fiber coil-winding for fiber-optic gyro manufacture [Text] / Thomas L. De Fazio', Kendall L. Belsley, Ronald H. Smith, Garry B. Shank, Jr., William H. Culver // Proceedings of the 1994 IEEE International Conference on Robotics and Automation, San Diego, CA, USA. – 1994. – vol. 1. –pp. 202-207, doi: 10.1109/ROBOT.1994.350987.
2. Sharon, Andre. Development of an automated fiber optic winding machine for gyroscope production [Text] /Andre Sharon, Stephen Lin// Robotics and Computer Integrated Manufacturing. – 2001. – vol. 17. – pp. 223-231, https://doi.org/10.1016/S0736-5845(00)00030-2
3. Zhang, Peng. The Design for Tension Control System of FOG Coil Winding [Text] / Peng Zhang, Ruifeng Yang, Xueliang Zhang // Applied Mechanics and Materials. -2013. – Vols. 380-384. – pp 317-320, doi:10.4028/www.scientific.net/AMM.380-384.317
4. Zhang, Peng. Compound Tension Control of an Optical-Fiber Coil System: A Cyber-Physical System View [Text] / Zhang Peng, Yang Rui-Feng, Zhang Xue-Liang // Advances in Mechanical Engineering. – 2014. – Article ID 204234. - 10 p., http://dx.doi.org/10.1155/2014/204234
5. Ge, Shuangchao. Constant Small Tension Control for Fiber Optic Coil Variable-Velocity Winding [Text] // Shuangchao Ge , Ruifeng Yang , Chenxia Guo // IEEE Access. – 2019. - vol. 7. - pp. 172012-172020, doi: 10.1109/ACCESS.2019.2956564
6. Ge, Shuang-Chao. A Highly Integrated Automatic Fiber Optical Gyroscope Sensing Coil Winding System /Shuang-Chao Ge*, Rui-Feng Yang, and Chen-Xia Guo // International Journal of Control, Automation and Systems. – 2021. – vol. 19, no. X. – pp/ 1-13, http://dx.doi.org/10.1007/s12555-020-0040-6
7. S. Ivanov Modeling of Influence of Shupe Effect on Fiber-Optic Goniometer with different coil winding types / Sergiy Ivanov, Pavlo Oliinyk, Gennadii Virchenko, Volodymyr Vanin and Mykola Tereschuk // Conference 2022 IEEE 3rd KhPI Week on Advanced Technology, 5pp. ISBN: 979-8-3503-9920-2.

УДК 621.39

УПРАВЛІННЯ МЕРЕЖЕЮ SDN З ВИКОРИСТАННЯМ КОНТРОЛЕРА Ryu

Бурлака Г.Ю.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: fastmotion1111@gmail.com

SDN NETWORK MANAGEMENT USING Ryu CONTROLLER

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.

Традиційні мережі обмежені рядом вимог до послуг, а також розміром мережі. Ці вимоги стосуються інженерного трафіку, керування потоком, реалізації політики, надійності, і деякі з них включають віртуалізацію. Мережі стають дедалі складнішими, їх важко проектувати та експлуатувати. Програмно визначена мережа (SDN) - це відносно нова мережева архітектура, яка стала найбільш обговорюваною мережевою технологією за останні роки та останньою розробкою в галузі цифрових мереж. Мета даної розробки - зробити ресурси більш керованими, безпечними та контрольованими [1].

SDN використовується, щоб зробити мережі більш програмованими та полегшити керування мережею. Це дозволяє традиційним мережам розділяти функції рівня керування та даних, створюючи більш динамічний, адаптований, автоматизований та керований дизайн. Мережа програмується за допомогою програмних додатків, які взаємодіють із пристроями рівня даних, які стають основними елементами пересилання та не мають прямого фізичного контролю над ними. Він відокремлює функціональність керування від інструменту мережевої площини та централізує його, маючи ефективне перенаправлення трафіку на відміну від традиційних мереж [2].

Архітектура програмно-конфігурованої мережі складається з трьох рівнів: додатків, управління та інфраструктури, пов'язаних один з одним через відкриті API-інтерфейси (рис. 1).

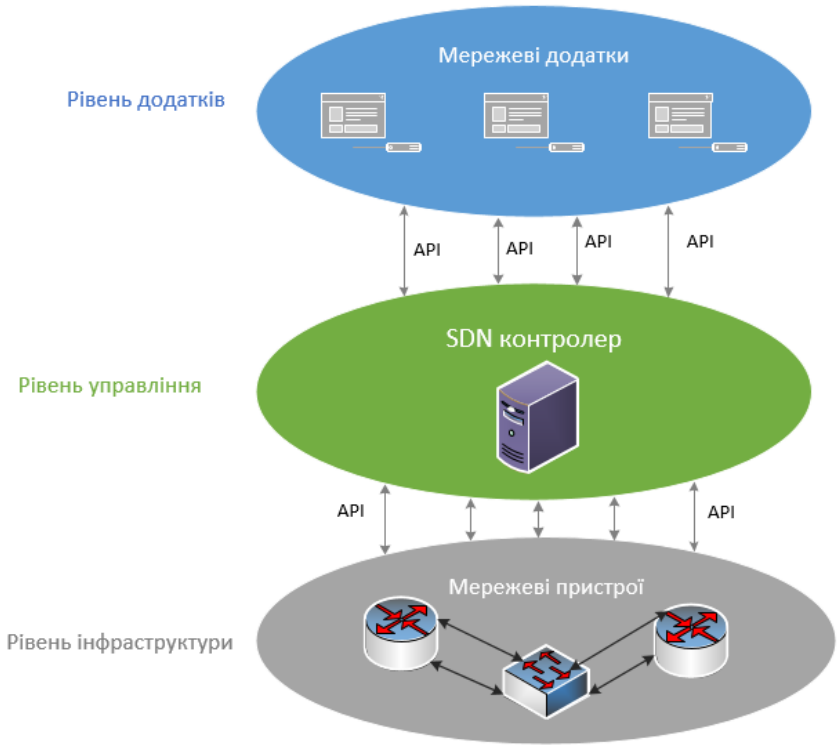


Рис. 1. Загальна архітектура SDN.

Ryu Controller - це відкритий контролер мережі (SDN), призначений для підвищення гнучкості мережі за рахунок посилення управління та адаптації способів обробки трафіку. В загальному, контролер SDN - це мозкова середовище SDN, що передає інформацію про комутатори та маршрутизатори за допомогою південних API, а також про програми та бізнес-логіку за допомогою північних API. Контролер Ryu підтримує NTT і також розвертається в обласних центрах обробки даних NTT.[3]

Контролер Ryu надає програмні компоненти разом із певними інтерфейсами прикладних програм (API), які сприяють розробникам створення нових додатків керування та контролю мережі. Цей компонентний підхід допомагає організаціям налаштувати розвертання відповідно до своїх конкретних потреб; Розробники можуть швидко і легко змінити існуючі компоненти або видалити свої власні, щоб базовий набір відповідав змінним вимогам їх програм.

Весь код Ryu повністю написаний на Python доступний під ліцензією Apache 2.0 і відкритий для всіх. Контролер Ryu підтримує протоколи управління мережею NETCONF і OF-config, а також OpenFlow, який є одним з перших стандартів зв'язку SDN, що найбільш широко використовуються.

Структура Ryu відрізняється від інших рішень тим, що вона надає просту допоміжну інфраструктуру, яку користувачі платформи повинні написати для використання на власний розсуд. Хоча для цього потрібний досвід розробки, це також забезпечує повну гнучкість рішення SDN. Існуючі компоненти можна швидко і легко оновлювати і об'єднувати в існуючі мережі, щоб задовольнити потреби різних програм, що змінюються, використовуючи ці компоненти. Завдяки своїм характеристикам Ryu є відмінним рішенням для невеликих комерційних та експериментальних

застосувань. Цей рівень керування дозволяє створювати програми та модулі, оскільки він розроблений на Python [4].

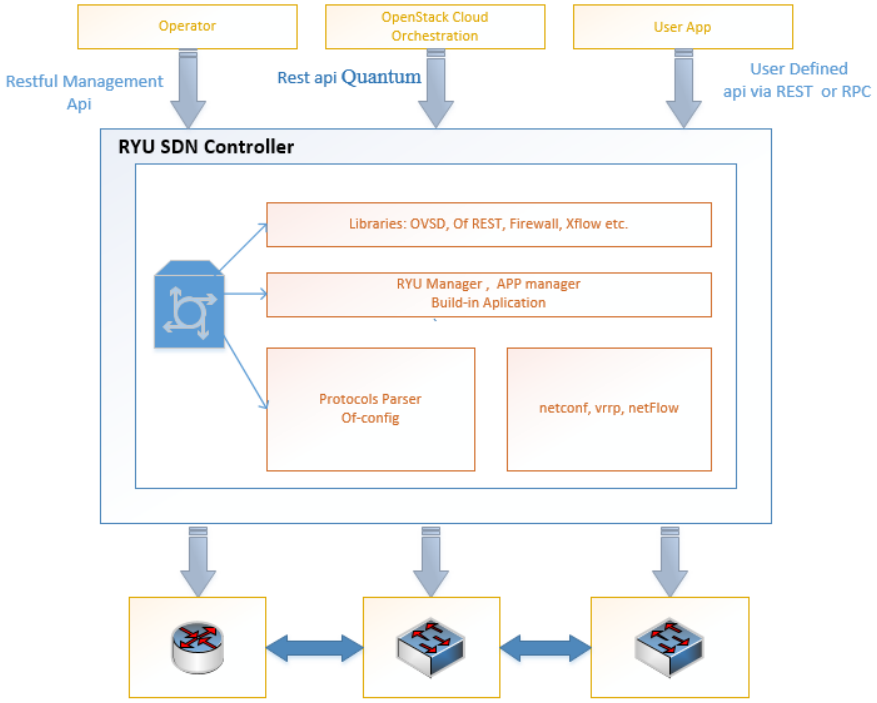


Рис. 2. Архітектура RYU Controller.

Контролер Ryu надає програмні компоненти разом із певними інтерфейсами прикладних програм (API), які сприяють розробникам створення нових додатків керування та контролю мережі. Цей компонентний підхід допомагає організаціям налаштувати розвертання відповідно до своїх конкретних потреб; Розробники можуть швидко і легко змінити існуючі компоненти або видалити свої власні, щоб базовий набір відповідав змінним вимогам їх програм. У майбутньому планується вивчити більше контролерів, щоб зменшити їх вплив на продуктивність SDN.

Література

1. 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.
2. Performance Analysis of Ryu-POX Controller in Different Tree-Based SDN Topologies [Електронний ресурс] — Режим доступу: https://www.researchgate.net/publication/354230822_Performance_Analysis_of_Ryu-POX_Controller_in_Different_Tree-Based_SDN_Topologies
3. Node to Node Performance Evaluation through RYU SDN Controller [Електронний ресурс] — Режим доступу: https://www.researchgate.net/publication/338703576_Node_to_Node_Performance_Evaluation_through_RYU_SDN_Controller
4. SDN Series Part Four: Ryu, a Rich-Featured Open Source SDN Controller Supported by NTT Labs. Controller [Електронний ресурс] — Режим доступу: https://thenewstack.io/sdn-series-part-iv-ryu-a-rich-featured-open-source-sdn-controller-supported-by-ntt-labs/

УДК 621.396

ВИКОРИСТАННЯ LI-FI В МЕДИЦИНІ

Чумаченко К.Д., Романов О.І.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: kchumachenko8@gmail.com

USE OF LI-FI IN MEDICINE

Currently, information technologies (IT) are implemented in virtually all areas of health care. That is why, medicine has acquired completely new features today. Li-Fi is a technology for transmitting data using light, which can be used in medicine to improve the quality of diagnosis and treatment.

LiFi, також відома як «Light Fidelity», — це технологія бездротової оптичної мережі, яка використовує світлодіоди для передачі даних. У 2011 році професор Гаральд Хаас зробив демонстрацію LiFi на TED (Technology, Entertainment, Design) Global Talk on Visible Light Communication (VLC). VLC використовує світло як середовище для забезпечення високошвидкісного зв'язку подібно до Wi-Fi.

LiFi — це система зв'язку у видимому світлі, яка передає бездротовий Інтернет-зв'язок на дуже високій швидкості. Це досягається шляхом дуже швидкого вмикання та вимикання світлодіода (мільйон разів на секунду). Завдяки цій технології світлодіодна лампочка випромінює імпульси світла і в межах цих випромінюваних імпульсів дані можуть передаватись до приймачів і з них.

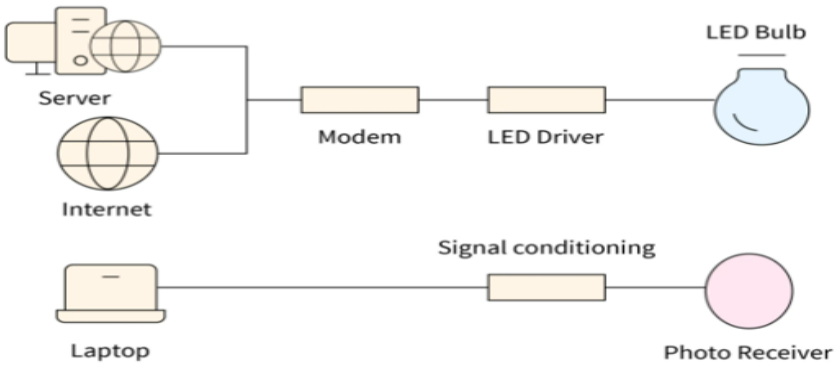


Рис.2. Передача даних за допомогою світла.

Отже, Li-Fi має два елементи, тобто передавальний елемент (світлодіод) і приймальний елемент (кремнієвий фотодіод). Світлодіод можна дуже швидко вмикати та вимикати, що дає чудову можливість для передачі даних у вигляді двійкового коду. Увімкнення світлодіоду є логічним 1 , а вимкнення світлодіоду логічним 0 . Дані кодуються в світлодіоди за допомогою контролера; після чого повинні варіювати, які світлодіоди

мерехтять залежно від даних, які ми хочемо закодувати, щоб отримати рядки з 0 і 1.

LiFi використовує видиме світло на відміну від радіочастот. Оскільки спектр видимого світла в 10 000 разів ширший за весь радіоспектр, LiFi тепер може використовувати більш повний діапазон доступних частот. Спектр видимого світла охоплює довжини хвиль від ближнього ультрафіолетового до ближнього інфрачервоного діапазону та частоти від 430 000 до 770 000 ГГц.

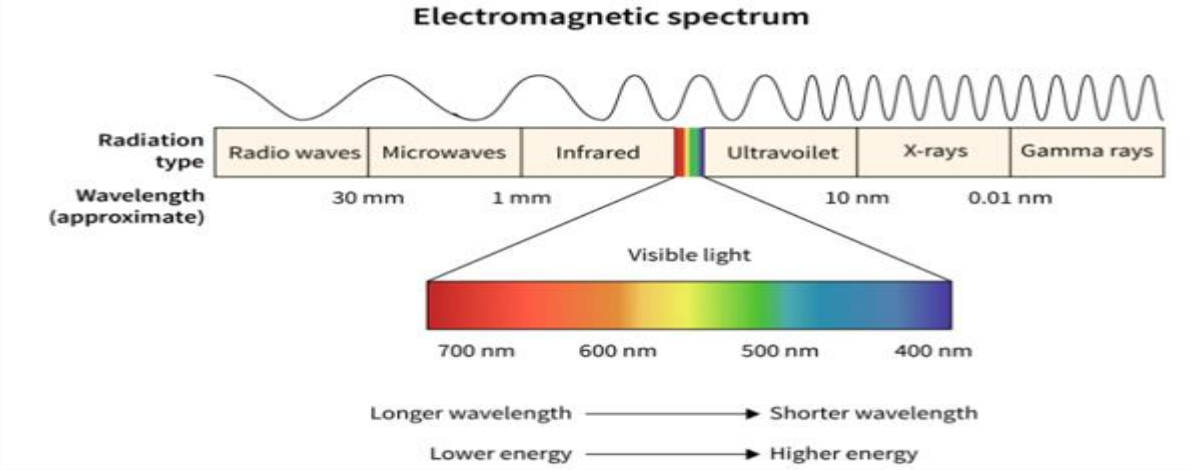


Рис.2. Електромагнітний спектр.

Ця технологія може бути корисною в багатьох сферах, включаючи медицину. Одним з головних переваг Li-fi є те, що вона не випромінює шкідливих радіаційних хвиль, тому, що на відміну від радіохвиль, світло безпечніше для людини, що може бути особливо корисно для пацієнтів з певними захворюваннями, такими як рак, також це становить загрозу для людей з серцевими імплантами, тощо.

Рис.3. Ілюстрація використання Li-fi в стоматології.

Li-fi може бути використана для передачі даних в лікарнях та клініках, де безпека даних та конфіденційність є особливо важливими. Світло не може проходити крізь стіни, тому дані не можуть бути зламані сторонніми особами, що забезпечує ще один рівень безпеки.

Крім того, технологія Li-fi може бути використана для створення точних терапевтичних систем, що дозволяє покращити ефективність лікування пацієнтів, також може бути використана для створення точкового освітлення в операційних залах, що допоможе хірургам більш точно проводити операції, та навіть в стоматології. Наприклад, якщо ми візьмемо до уваги стоматологію, то Li-fi може бути використана для передачі даних з медичних приладів, таких як рентгенівські апарати та інші діагностичні прилади, що дозволяє лікарям збирати точні дані про стан зубів, або та допомагати у виборі оптимального лікування.

Іншим прикладом використання Li-fi може бути створення системи контролю за гігієною ротової порожнини. За допомогою Li-fi можна створити систему, яка буде автоматично контролювати гігієну ротової порожнини пацієнта, тим самим зменшуючи ризик захворювань та покращуючи стан зубів та ясен.

За допомогою Li-fi можна створити систему, яка буде автоматично контролювати дозу ліків, що надходять до пацієнта, тим самим зменшуючи ризик передозування та покращуючи ефективність лікування. Електронна автоматизована підготовка призначень, рецептів, виписок, лікарняних листів та інших стандартизованих документів для пацієнтів.

Отже, використання технології Li-fi в стоматології може мати значний позитивний вплив на ефективність лікування пацієнтів та забезпечення безпеки даних.

Література

1. IT ТЕХНОЛОГІЇ В МЕДИЦИНІ [Електронний ресурс] — Режим доступу: https://naukam.triada.in.ua/index.php/konferentsiji/42-dvanadtsyata-vseukrajinska-praktichno-piznavalna-internet-konferentsiya/462-it-tekhnologiji-v-meditsini
2. What exactly is LiFi? [Електронний ресурс] — Режим доступу: https://lifi.co/what-is-lifi/
3. LiFi vs WiFi [Електронний ресурс] — Режим доступу: https://www.scaler.com/topics/lifi-vs-wifi/
4. Mehmet Güven, Erdal Eroğlu, Selçuk Çömlekçi. Electromagnetic Fields in Dental Clinics. Am J Biomed Sci & Res. 2021 - 13(5). AJBSR.MS.ID.001902. DOI: 10.34297/AJBSR.2021.13.001902.
5. Інформаційні технології в медицині [Електронний ресурс] — Режим доступу: https://uk.wikipedia.org/wiki

УДК 621.39

ЯКІСТЬ ОБСЛУГОВУВАННЯ НА ОСНОВІ SIP

Підпалий О.І.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: studentalex2515@gmail.com

QUALITY OF SERVICE BASED ON SIP

Analysis, optimization and control of quality of service (QoS) parameters such as delay, jitter, packet loss rate and throughput for SIP-based communication services.

Аналіз, оптимізація та контроль параметрів якості обслуговування (QoS), таких як затримка, джиттер, швидкість втрати пакетів та пропускна здатність для послуг зв'язку на основі SIP.

Постановка задачі. Задана якість обслуговування (Quality of service – QoS) може вводитися в мережах, щоб визначити здатність мереж відповідати заданим вимогам. За допомогою якості обслуговування можна визначити, чи може мережа виконати завдання з моніторингу, обробки та передач даних при різних умовах функціонування. Тому доцільно провести аналіз параметрів якості обслуговування (QoS) та методів забезпечення якості обслуговування для сенсорних мереж, визначити їх основні переваги та недоліки, а також проаналізувати чи доцільно їх застосовувати для тактичних безпроводових сенсорних мереж.

Аналіз останніх публікацій. Щодо проблематики параметрів якості обслуговування (QoS) та методів забезпечення якості обслуговування для сенсорних мереж варто відзначити роботи О.В. Лемешка, В.В. Петрова, Б.С.Цибакова, А.Г. Ложковського, О.І.Сидорової, Yanfeng Zhang, Cuirong Wang та Yuan Gao.

Метою статті є аналіз існуючих параметрів підвищення якості показників передачі трафіку та методів забезпечення QoS в безпровідних мережах.

Виклад основного матеріалу. Найбільшим актуальним науковим завданням у галузі телекомунікацій є передача потокового трафіку в режимі реального часу з дотриманням певних вимог щодо якості обслуговування. Це можна пов'язати з тим, що потоки даних передаються по мережі, ресурси якої розподіляються між потоками за певними пропорціями. Оскільки дані, які можуть передаватися, різні за своїми параметрами, то потрібно мати механізм, який дасть змогу розв'язати задачу щодо розподілення ресурсів дуже швидко, відповідно до властивостей потоку, який передається у конкретний час через конкретний телекомунікаційний вузл. Такий механізм повинен грунтуватись на вдосконалення методів розподілу ресурсу, що має високу масштабованість, швидкодію, гнучкість, низькі операційні складності та ресурсоємності.

Для підвищення якості обслуговування (QoS) переданих мережевних трафіків актуальним є пошук гнучкого методу керування мережним ресурсом для забезпечення їхніх збалансованих завантажень й гарантованої якості обслуговування різних трафіків користувачів у мультисервісній мережі [1].

Якість обслуговування (Quality of Service, QoS) визначає кількісну оцінку імовірності того, що через мережу будуть передаватися певні потоки даних між двома вузлами відповідно до потреб додатку або користувачів. QoS є необхідним для пакетної мережі, яка використовується для сервісу людей у режимі реального часу, насамперед VoIP. Мережевий протокол, який обслуговує сервіс реального часу є чутливий до обслуговування, а саме до втрати пакету даних, затримки у передачах пакетів та нерівномірності цієї затримки.

У більшості випадків якість зв'язку характеризується чотирма параметрами [2]:

- Пропускна смуга, в якій описується доступна пропускна здатність каналу зв'язку. Вимірюється у бітовій швидкості - bit/s, kbit/s, Mbit /s.
- Затримка при передачі пакетів, вимірюється у мілісекундах.
- Джиттер (Jitter) - нерівномірна затримка пакету при передачі цих пакетів.
- Втрата пакетів (Packet loss) - визначає кількість пакетів, які були загублені у мережі під час передачі.

Для простоти розуміння канал зв'язку можна уявити у вигляді традиційної труби, а пропускну здатність можна описати як функцію двох параметрів: ширини та довжини труби. Коли передача даних стикається з проблемою «вузького місця» надсилання та отримання пакетів маршрутизаторами, зазвичай використовується метод FIFO: First In - First Out (Першим зайшов - першим вийшов) [3].

Для щільного трафіку це створює перевантаження трафіку, і рішення просте: усі пакети, які не потрапляють у чергу FIFO (вхідні чи вихідні), ігноруються маршрутизатором і тому втрачаються безповоротно. Розумним підходом є використання «розумних» черг, де пріоритет пакетів залежить від типу послуги - ToS (Type of Service). Необхідна умова: пакети вже повинні бути позначені типом служби, щоб створити «розумну» чергу. Звичайні користувачі найчастіше зустрічають термін QoS в домашніх маршрутизаторах, які підтримують QoS. Наприклад, логічно надати високий пріоритет VoIP і низький пріоритет FTP, SMTP клієнтам мережі обміну файлами. На відміну від класичних (бездротових або дротових) мереж, бездротові сенсорні мережі забезпечують не тільки передачу даних, а й збір і обробку даних. Відповідно, якість обслуговування та його показники в бездротових сенсорних мережах також будуть відрізнятися від класичних уявлень.

Тактичні сенсорні мережі характеризуються: I – обмеженими ресурсами вузла мережі (щодо продуктивності процесора, пам’яті, потужності передавача, заряду батареї, обмеженої дальності та пропускної

здатності каналів радіозв'язку між вузлами, концентрації трафіку біля шлюзів тощо) II – характеристики операції (розгортання вузлів (випадкове, детерміноване), випадкові зміни топології (переміщення вузлів, руйнування вузлів, розряд батареї), резервування даних (через щільне розташування вузлів), транспортування різних типів трафіку, велика масштабованість мережі (сотні датчиків), розгортання та експлуатація мережі в раніше невідомій географічній місцевості, де ворог може завдати шкоди) [4].

Є такі традиційні методи надання QoS, як використання протоколів з функціями QoS: EART (Energy-aware QoS Routing), протокол використовується для передачі трафіку в реальному часі, використовується для збалансування енергоспоживання вузлів і розширення циклу роботи мережі, а також вибору маршруту з більшим енергозбереженням. Запропонований протокол враховує параметри маршрутизації QoS, затримку та підвищену надійність.

EQSR (Efficient and QoS-Aware Multipath Routing Protocol) призначений для побудови маршрутів за наявності затримок повідомлень. В основному він використовує механізм протоколу спрямованої дифузії. На етапі пошуку шляху вартість кожного з'єднання використовується як індекс. При побудові маршруту потрібно врахувати значення відношення сигнал/шум, буферну ємність вузлів і залишок енергії акумулятора [5].

SAR (Sequential Assignment Routing) - один із найперших протоколів маршрутизації в бездротових сенсорних мережах. Він заснований на визначеному пріоритеті для кожного пакета. Крім того, підключення та маршрути включають міру їх здатності надавати якісні послуги. Цей показник визначається затримкою та споживанням енергії. На основі цього алгоритму створюється дерево маршрутизації. Для цього враховується кілька параметрів, таких як пріоритет пакетів, енергія, показники QoS. Протокол періодично оновлює маршрути на основі стану мережі.

SPEED (Stateless Protocol for Real-Time Communication in Sensor Networks) Кожен вузол зберігає інформацію про своїх сусідів і дані про своє географічне розташування, щоб знайти шляхи передачі. Крім того, протокол намагається гарантувати, що кожен пакет має певну швидкість передачі [6].

Таким чином, можна заздалегідь оцінити затримку транзиту посилки від відправника до одержувача, розділити відстань на швидкість посилки тощо.

Перевагою використання вищезазначеного протоколу є гарантія енергозбереження та забезпечення якості обслуговування на рівні мережі. Недоліком є те, що ці протоколи зосереджені лише на певних типах трафіку та потребують меншого розміру мережі [7].

Можна зазначити, що надання QoS у сенсорних мережах досягається завдяки взаємодії трьох аспектів: покриття, моніторинг і передача даних. Тому, пропонується введення крос-рівневої надбудови над рівнями OSI, яка буде здійснювати узгодження та координацію рівнів моделі передачі даних та всіх функцій системи управління (покриття, моніторинг і передача даних) БСМ.

Необхідність переходу на крос-рівневу модель зумовлюється: – з'єднання окремих та ізольованих механізмів QoS може спричинити конфлікти в забезпеченні заданої якості обслуговування; – забезпечення QoS окремо для кожного з рівнів є неефективним рішенням; – задана якість обслуговування, яка підтримується на окремому рівні моделі взаємодії не може гарантувати загальне забезпечення QoS.

Висновок. Тому на даний момент розроблено велику кількість методів для покращення та забезпечення QoS у бездротових сенсорних мережах. Проведений аналіз показує, що методи, які використовуються в традиційних бездротових (або дротових) мережах, не можуть бути ефективно використані в бездротових сенсорних мережах, враховуючи відмінності в характеристиках цих мереж. Проведені дослідження показують, що не існує методу, який міг би врахувати всі параметри сенсорних мереж і повністю забезпечити QoS.

Тому в цій статті пропонується новий метод оцінки якості обслуговування BSM, тобто оцінки трьох основних функцій бездротових сенсорних мереж: покриття, моніторинг і передача даних.

Напрямок подальших досліджень полягає у вдосконаленні існуючих методів покращення та гарантування якості обслуговування, а також їх застосування в тактичних сенсорних мережах та визначенні напрямків подальших наукових досліджень.

Література

1. Kabara, K.; Calle, M. MAC protocols used by wireless sensor networks and a general method of performance Evaluation. Int. J. Distrib. Sens. Netw. 2018, 1 – 11.
2. Sohrabi, K., Gao, J., Ailawadhi, V., and Pottie, G. J. Protocols for self organization of a wireless sensor network. IEEE Personal Communication Magazine 77 (October 2019), 16 – 27.
3. Reason, J. M., and Rabaey, J. M. A study of energy consumption and reliability in a multi-hop sensor network. SIGMOBILE Mob. Comput. Commun. Rev. 8, 1 (2020), 84 – 97.
4. Жук О.В. Моделі побудови покриття і виявлення цілей в безпроводових сенсорних мережах. / О.В. Жук, В.А. Романюк, В.В. Тарасов, Д.В. Ткаченко // Збірник наукових праць ВІТІ. – 2018. № 3. – С. 66 – 75.
5. Polschykov K. Methods and Technologies Analysis of The Real-Time Traffic Transmission Requests Servicing / K. Polschykov, K. Kubrakova, O. Odaruschenko // World Applied Programming. – Vol. 3, Issue 9. – 2022. – P. 446 – 450.
6. Романчук В. І. Аналіз структури мережевого трафіку та мережевих аномалій на прикладі сегмента локальної мережі кампусу Національного університету "Львівська політехніка"/ В. І. Романчук, С. В. Алексєєв, В.В. Червенець, Р. С. Колодій // Радіоелектроніка та телекомунікації [зб. наук. пр.] / відп. ред. Б.А. Мандзій. – Л. : Вид-во Нац. ун-ту "Львів. політехніка", – 2018. - № 796. – С. 157–163. (Index Copernicus, Google scholar).
7. Бугиль Б.А. Методи оптимізації фізичної та логічної структур телекомунікаційних мереж / О.А. Лаврів, Б.А. Бугиль, В.В. Червенець, М. І. Бешлей // Радіоелектроніка та телекомунікації [зб. наук. пр.] / відп. ред. Б.А. Мандзій. – Л. : Вид-во Нац. ун-ту "Львів. політехніка", – 2019. – № 766. – С. 76 – 81. (Index Copernicus, Google scholar).

УДК 621.391

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРОДУКТИВНОСТІ СУЧАСНИХ ПРОГРАМНИХ КОМУТАТОРІВ

Берестовенко О.О., Маньківський В.Б.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: o.berestovenko@kpi.ua, v.b.mankivskiy@gmail.com

COMPARATIVE ANALYSIS OF THE PRODUCTIVITY OF MODERN SOFTWARE SWITCHES

In recent years, Network Function Virtualization (NFV) has become increasingly popular as a way to replace proprietary hardware appliances with Virtual Network Functions (VNFs) implemented in software. To effectively route traffic between VNFs and physical Network Interface Cards (NICs), it is essential to compare the performance of different software switch designs and architectures. This paper proposes a comprehensive methodology for this comparison, exploring the design spaces of four state-of-the-art software switches and evaluating their performance under four representative test scenarios.

Звичайний комутатор — це пристрій, який дозволяє з'єднувати мережеві пристрої і відправляти мережевий трафік на потрібні порти. Програмні комутатори будуються на базі програмного забезпечення, яке дозволяє перетворити звичайний сервер в комутатор. Вони працюють на основі відкритих протоколів мережі, що дозволяє їм працювати з різноманітним обладнанням та програмним забезпеченням. Програмний комутатор має спеціальні драйвери, які дозволяють йому працювати з фізичними мережевими інтерфейсами, а також програмне забезпечення, що забезпечує обробку трафіку та передачу його по мережі. Всі ці елементи дозволяють програмному комутатору працювати як звичайний комутатор, але з додатковими можливостями конфігурації та моніторингу роботи мережі [1].

Розглянемо та порівняємо чотири програмних комутатора: FastClick, OVS-DPDK, Snabb та VPP. Порівнювалися саме ці комутатори, оскільки вони є представниками різних підходів до проектування віртуальних комутаторів, які використовуються в області віртуалізації мережі. Ці комутатори є популярними та широко використовуються у віртуалізованих середовищах [2].

Крім того, кожен з цих комутаторів має свої особливості та переваги в певних сценаріях використання. Порівняння цих комутаторів дозволяє зрозуміти, які підходи до проектування віртуальних комутаторів є більш ефективними в різних сценаріях використання та дозволяє знайти найбільш підходящий комутатор для конкретного використання. Розглянемо їх особливості детальніше:

FastClick - це програмний комутатор, який дозволяє використовувати мову програмування C++ для створення правил обробки мережевого трафіку який працює на рівні ядра операційної системи та надає можливість програмувати маршрутизацію, фільтрацію та обробку пакетів за допомогою

спеціальної мови програмування. Основна перевага FastClick полягає в його гнучкості та програмованості. Розроблений як проект Массачусетського технологічного інституту який має назву Click Modular Router Project був спочатку розроблений для побудови спеціалізованих маршрутизаторів та комутаторів, але в подальшому був адаптований для використання в хмарних середовищах [3].

OVS-DPDK - це програмний комутатор на базі Open vSwitch, який використовує Data Plane Development Kit (DPDK) для прискорення обробки мережевого трафіку. OVS-DPDK використовує розподілену архітектуру, яка дозволяє виконувати функції комутатора на рівні додатку, що дозволяє забезпечувати високу пропускну здатність та низьку затримку. Розроблений VMware та Linux Foundation спеціально для використання у віртуалізованих середовища і має високу продуктивність завдяки використанню технології Data Plane Development Kit (DPDK) [4].

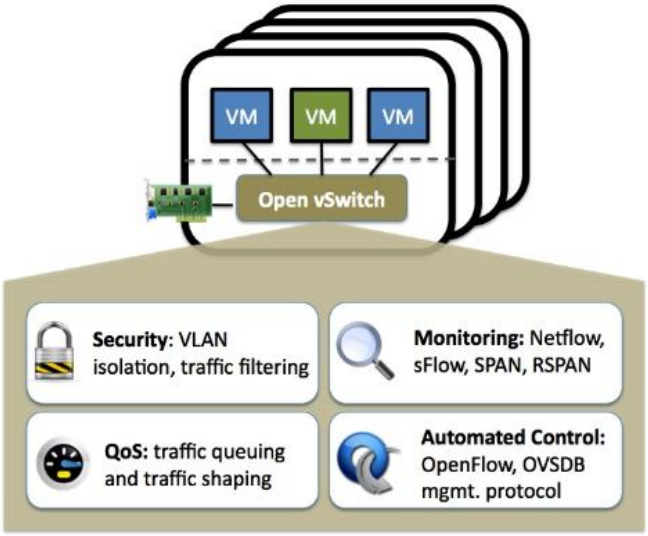


Рис.1 Коммутатор OVS-DPDK.

Snabb - це програмний комутатор, який був розроблений спеціально для використання в вимогливих застосунках мережевої віртуалізації. Snabb пропонує відкриту архітектуру для розробки додатків та можливість використання мов програмування, таких як C та Lua. У порівнянні з іншими комутаторами у цьому дослідженні, Snabb має найнижчу затримку, що робить його відміним вибором для застосувань з вимогами до низької затримки. Однак, Snabb має меншу пропускну здатність порівняно з OVS-DPDK. Розроблена добровольцями із Snabb Community він був розроблений з метою забезпечення високопродуктивного мережевого з’єднання віртуальних машин, але може бути застосоване для реалізації різних мережевих функцій [5, 7].

VPP - використовує відкриту архітектуру та пропонує можливості для налаштування та оптимізації обробки мережевого трафіку. VPP має дуже високу пропускну здатність та низьку затримку. Однак, в порівнянні з іншими комутаторами у цьому дослідженні, VPP вимагає більше ресурсів для обробки мережевого трафіку. Розроблений компанією Linux foundation

backed на основі технології Vector Packet Processing. Щоб забезпечить масштабованість мереж, VPP зчитує найбільший доступний сектор пакетів на рівні мережевого вводу-виводу. Замість того, щоб обробляти кожен пакет окремо по всьому графу з кількома вузлами, VPP вибирає весь вектор пакетів і проштовхує їх через вузол графу, перш ніж перейти до наступного вузла. Потім кеш інструкцій адаптується до процесу, а пакети, що залишилися, обробляються ще швидше завдяки раніше вивченим інструкціям з першого векторного пакета.

Кожен з програмних комутаторів має свої переваги та недоліки в залежності від конкретного застосування. Наприклад, якщо важливо досягнути максимальної пропускної здатності та мінімальної затримки, то варто використовувати OVS-DPDK або VPP [6, 8]. Якщо ж необхідна більш гнучка конфігурація та налаштування, то можна використовувати Click або Snabb. Крім того, вибір програмного комутатора може залежати від характеристик обчислювальних ресурсів та мережевого обладнання, що використовується.

Кожен комутатор, що реалізований в програмному забезпеченні, або пристрій для тестування (DUT), оцінюється за 2 різними тестовими сценаріями: фізичний NIC до фізичного NIC (p2p), VNF до VNF (v2v) як ілюстровано на рис. 2. Потоки даних 2 сценаріїв пояснюються наступним чином:

(p2p) фізичний до фізичного: у цьому сценарії пакети надходять через фізичний NIC, отримує пристрій для тестування та пересилаються через інший NIC. Вимірювання проводяться на джерелі та приймачі потоку пакетів, поза пристроєм для тестування. Це найпростіший тестовий сценарій без VNF, що працюють у віртуальному середовищі, і надає базові результати для всіх програмних комутаторів.

(v2v) virtual-to-virtual: У випадку v2v пакети генеруються джерелом VNF та вводяться в пристрій для тестування. Потім він пересилає пакети у приймач VNF для вимірювання. Цей сценарій демонструє ефективність пристроїв щодо пересилання трафіку між VNF.

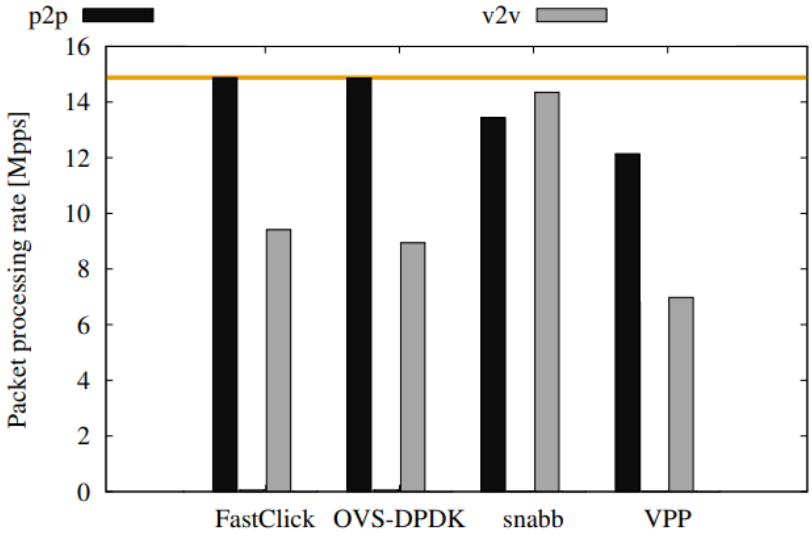


Рис.2: Результати тестів пропускної здатності для всіх сценаріїв.

Віртуальна машина дозволяє максимум надсилати 14,9 млн пакетів на секунду для пакетів розміром 64 Б.

Результати дослідження. На рис. 2 показана одностороння пропускна здатність розглянутих програмних комутаторів у сценаріях, описаних вище. Як ми можемо побачити, жоден програмний комутатор не переважає в розглянутих сценаріях. Наприклад Snabb виявляється кращим у сценарії v2v, оскільки його реалізація vhost-user є більш ефективною для доставки пакетів між віртуальними машинами.

На основі результатів дослідження можна зробити висновок, що Snabb має найкращу продуктивність серед усіх програмних комутаторів для віртуалізації функцій мережі. Проте, враховуючи важливість затримки для деяких додатків, OVS-DPDK може бути кращим вибором випадку коли будуть розглядатися мережі із фізичними та віртуалізованими функціями мережі. Крім того, важливо враховувати розмір буферів для оптимальної продуктивності.

Різні підходи до проектування віртуальних комутаторів дозволяють вирішувати різні завдання в області віртуалізації мережі. Наприклад, FastClick може бути корисним для налагодження тестових середовищ, тоді як OVS-DPDK може забезпечити високу пропускну здатність для обробки великої кількості трафіку. Snabb може бути корисним для використання в телекомунікаційних мережах, тоді як VPP може бути корисним для використання в хмарних середовищах та мережах інтернету речей.

Література

1. H. Song, X. Zuo, and L. Liu, "A Comprehensive Survey on Software-Defined Networking," Journal of Network and Computer Applications, vol. 135, pp. 23-35, 2019.
2. N. K. Yadav, P. Patil, R. Poddar, and R. Buyya, "Performance Benchmarking of State-of-the-Art Software Switches for NFV," IEEE Access, vol. 8, pp. 37374-37390, 2020.
3. The Click Modular Router https://github.com/kohler/click
4. Open vSwitch Project, "Open vSwitch," [Online]. Available: http://www.openvswitch.org.
5. Snabb https://github.com/snabbco/snabb
6. "Performance Comparison of OVS and VPP on High-Performance Networking" by Hyunwoo Nam, Eunji Lee, Sangwon Hyun, and Taesoo Kwon, published in the IEEE Access Journal in 2019.
7. Романов О.І., Свид І.В., Корнієнко Н.І., Романов А.О. Управління оптичною мережею контролером SDN на базі ONOS//Радіотехніка, № 210, 2022, С.188-196, DOI:10.30837/rt.2022.3.210.16
8. Romanov, O., Nesterenko, M., Mankivskyi, V., Zhuk, O. Principles of Building Modular Control Plane in Software-Defined Network//Lecture Notes in Networks and Systems, 2023, 548, pp. 333–355, DOI: 10.1007/978-3-031-16368-5_17 https://link.springer.com/chapter/10.1007/978-3-031-16368-5_17

УДК 621.395

ПЕРЕВАГИ ПРОГРАМНОГО КОМПЛЕКСУ З АРХІТЕКТУРНИМ ПАТТЕРНОМ SIDE-EFFECT З ISTIO

Маньківський В.Б., Мінжинер Н.М.
Навчально-науковий Інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: v.b.mankivskiy@gmail.com , minzinernina@gmail.com

ADVANTAGES OF THE SOFTWARE COMPLEX WITH SIDE-EFFECT ARCHITECTURAL PATTERN BASED ON ISTIO

This article examines the software complex for managing the network of services, its advantages and disadvantages. The side-effect architectural complex used in ISTIO to separate functions is described.

У роботі розглянуто програмний комплекс для управління мережею сервісів, його переваги і недоліки. Описано архітектурний комплекс side-effect, який використовується в ISTIO для розділення функцій.

ISTIO - це відкритий програмний комплекс для управління мережею сервісів, який дозволяє керувати трафіком, забезпечувати безпеку та відстежувати метрики в середовищах мікросервісної архітектури. ISTIO забезпечує зручний та простий спосіб налаштування, моніторингу та управління взаємодії між сервісами.

Одним із ключових архітектурних паттернів, які використовуються в ISTIO, є side-effect паттерн. Він використовується для розділення функцій на дві категорії: ті, що залежать від зовнішнього середовища, та ті, що не залежать від нього. Функції, які залежать від зовнішнього середовища, повинні бути забезпечені додатковими заходами безпеки та надійності, так як вони можуть піддаватися різноманітним впливам зовнішнього середовища.

Side-effect паттерн дозволяє розділяти функції на дві групи та забезпечувати їх незалежність від зовнішнього середовища. Це дозволяє зменшити залежність між сервісами та забезпечувати безпеку та надійність системи. Крім того, side-effect паттерни дозволяє забезпечувати масштабованість та ефективність системи. Функції, які не залежать від зовнішнього середовища, можуть бути кешовані або розподілені між декількома вузлами системи, що дозволяє збільшити продуктивність та зменшити навантаження на окремі вузли.

ISTIO також забезпечує безпеку мікросервісної архітектури за допомогою таких механізмів, як автентифікація, авторизація та шифрування трафіку. ISTIO може використовувати різні методи автентифікації, такі як JWT або X.509 сертифікати, щоб забезпечити безпеку між сервісами. Крім того, ISTIO може використовувати політику авторизації, щоб дозволяти або забороняти доступ до сервісів в залежності від прав доступу користувача.

ISTIO також забезпечує моніторинг та логування мікросервісної архітектури, може збирати метрики про роботу сервісів та розподілені траси

для діагностики проблем у мікросервісах.

Однією з головних переваг ISTIO є його здатність автоматично налаштовувати та управляти мікросервісною архітектурою. ISTIO може використовувати правила маршрутизації, щоб автоматично розподіляти трафік між сервісами, а також виконувати балансування навантаження.

Однією з альтернатив ISTIO для автоматичного розподілу трафіку між мікросервісами є Kubernetes Ingress. Це механізм, який дозволяє управляти зовнішнім доступом до сервісів Kubernetes-кластера. Kubernetes Ingress може розподіляти трафік між різними сервісами, використовуючи правила маршрутизації на основі URL-адрес, хост-імен, заголовків тощо. Однак, в порівнянні з ISTIO, Kubernetes Ingress має менші можливості для управління мережею та безпекою.

Можна порівняти Kubernetes Ingress і ISTIO за наступними параметрами:

- Функціональність: ISTIO має більш широкий набір функцій, що дозволяє управляти мережею та безпекою на рівні мікросервісів. Kubernetes Ingress надає лише базові можливості маршрутизації.

- Складність налаштування: ISTIO вимагає більше зусиль для налаштування, оскільки має складну архітектуру та більше можливостей. Kubernetes Ingress має меншу складність налаштування, що може бути корисним для простих проектів.

- Швидкодія: Kubernetes Ingress може бути швидшим за ISTIO, оскільки не має додаткових шарів мережевої абстракції.

- Масштабованість: ISTIO може бути більш масштабованим за рахунок своєї більш детальної конфігурації мережі та безпеки.

- Ресурсоємність: ISTIO вимагає більше ресурсів для роботи, оскільки має більш складну архітектуру. Kubernetes Ingress може працювати з меншою кількістю ресурсів.

- Підтримка: ISTIO має більш активну спільноту та підтримку, оскільки є більш популярним рішенням для управління мережею та безпекою в середовищі мікросервісів.

- Зручність використання: для простих проектів, Kubernetes Ingress може бути більш зручним у використанні, оскільки має меншу складність налаштування та відповідає базовим потребам в управлінні мережею.

Кількісні показники, за якими можна оцінювати ці два підходи:

1. Швидкість відповіді системи: час, який затрачується на виконання запитів і повернення результатів користувачам.

2. Надійність: частота виникнення помилок в системі, таких як відмови мікросервісів або помилки маршрутизації трафіку.

3. Масштабованість: здатність системи до збільшення обсягів трафіку, кількості користувачів і мікросервісів.

4. Потужність обчислювальних ресурсів: кількість ресурсів, необхідних для забезпечення роботи системи.

5. Витрати на розробку та підтримку: кошти, необхідні для створення та підтримки системи з використанням певного підходу.

6. Відкритість та легкість використання: чи є підхід відкритим та чи легко зрозуміти та використовувати для розробників.

7. Рівень складності системи: якість і час, необхідні для впровадження певного підходу.

Кількість вхідних запитів	*K8s Ingress масштабування*	*Istio масштабування*
100	1000 мс	1000 мс
200	1400 мс	1000 мс
500	2450 мс	1000 мс
1000	4278 мс	1000 мс
2000	7658 мс	2000 мс
5000	14933 мс	5000 мс

Результати проведені на математичному моделюванні двох підходів: Використання традиційного підходу з HTTP протоколом. Вхідні дані: час на обробку запиту складає 500 мілісекунд, а час на передачу даних від клієнта до сервера і назад складає 200 мілісекунд.

Використання ISTIO для автоматичного розподілу трафіку між сервісами: середній час на обробку запиту становить 400 мілісекунд, а час на передачу даних між сервісами складає 50 мілісекунд. Для ручного масштабування припускається, що обидва сервіси мають по одному екземпляру.

Висновок. Щоб підсумувати, ISTIO є потужним та важливим інструментом для управління мікросервісною архітектурою, який забезпечує безпеку, масштабованість та надійність системи, підтримку для різних платформ та хмарних сервісів, активну спільноту та прозорість мікросервісної архітектури. Незважаючи на деякі недоліки, ISTIO може допомогти організації зменшити витрати на розробку та підтримку системи та забезпечити ефективний розвиток та масштабування.

Література

1. Barré, J. and Garcia-Molina, H. "Performance analysis of Istio as a service mesh for microservices." Journal of Systems and Software, vol. 157, 2019, article no. 110425. doi: 10.1016/j.jss.2019.110425.
2. Dang, H., Yang, Y., Zheng, Z., Liu, X., and Zhou, W. "Deploying Istio Service Mesh in Kubernetes: A Comprehensive Guide." IEEE Access, vol. 8, 2020, pp. 77312-77325. doi: 10.1109/access.2020.2981468.
3. Gil, Y. and Kim, H. "Performance evaluation of service mesh using Istio for container-based applications." Journal of Parallel and Distributed Computing, vol. 133, 2019, pp. 175-185. doi: 10.1016/j.jpdc.2019.07.002.
4. Gong, Y. and Wang, Y. "Deploying Istio in Kubernetes with enhanced security." Journal of Ambient Intelligence and Humanized Computing, vol. 11, no. 6, 2020, pp. 2313-2323. doi: 10.1007/s12652-019-01674-5.
5. Meng, Y., Wang, X., Lu, S., Zhou, W., and Liu, X. "Improving microservice communication with Istio service mesh." IEEE Access, vol. 8, 2020, pp. 5364-5374. doi: 10.1109/access.2019.2966888.

УДК 621.391

РОЗГОРТАННЯ ONOS КЛАСТЕРУ ДЛЯ ЕМУЛЯЦІЇ РОБОТИ КОРИСТУВАЦЬКОЇ МЕРЕЖІ SDN

Романов О.І., Сколець С.С., Марінов А.І
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: a_i_romanov@ukr.net, serskols@gmail.com, anton_marinov@ukr.net

ONOS CLUSTER DEPLOYMENT FOR EMULATION OF CUSTOM SDN NETWORK

This article outlines the process of building a custom network based on an ONOS cluster, which involves deploying ONOS controllers and installing them on cluster nodes, creating a virtual user network, configuring and managing network services and traffic on ONOS using a graphical interface or API, collecting and analyzing network data to verify network operation.

У даній статті відображено процес побудови користувацької мережі на базі ONOS кластеру, що передбачає розгортання контролерів ONOS та встановлення їх на вузлах кластеру, створення віртуальної користувацької мережі, налаштування та керування мережевими сервісами та трафіком в ONOS з використанням графічного інтерфейсу або API, збір та аналіз мережевих даних з метою перевірки роботи мережі.

Побудова користувацької мережі на базі ONOS та Mininet має на меті дослідження та тестування різноманітних мережевих сценаріїв. Мінімізуючи витрати на обладнання, можна створити віртуальну мережу, що дозволить вирішити проблеми на різних рівнях мережі. Також даний підхід дозволяє проводити дослідження та тестування різних аспектів мережевих технологій, таких як розподілені протоколи маршрутизації, стратегії керування трафіком, збір статистики про мережу та інші.

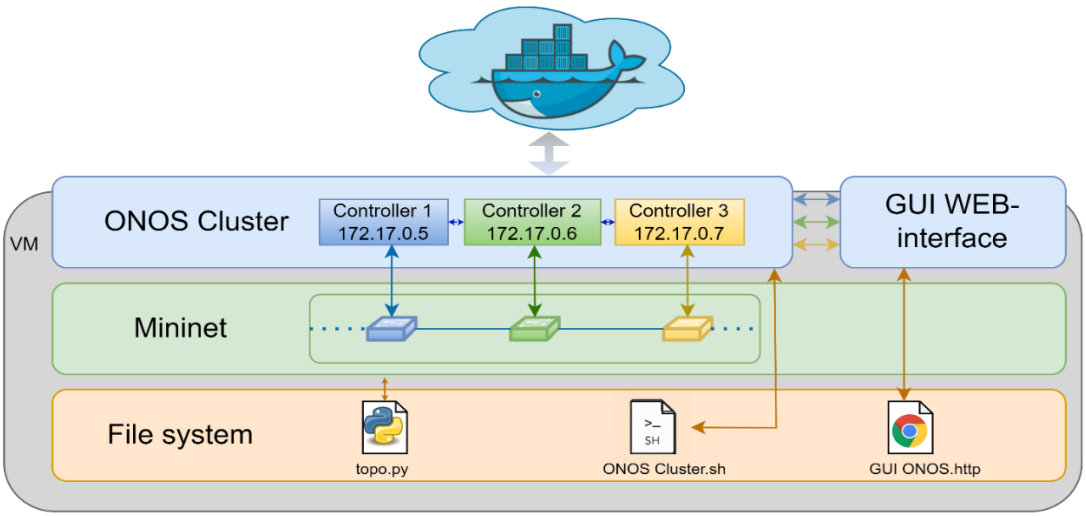


Рис.1. Програмні компонентів мережі на базі ONOS кластеру.

Це дає можливість вирішити проблеми, пов'язані з недостатньою ефективністю та надійністю мережі, виявити проблеми в роботі мережі та знайти їх вирішення, визначити місця заторів та вузькі місця, що може допомогти зробити мережу більш ефективною та надійною. Крім того, це дозволяє відтворити різні сценарії, що можуть статися в реальних мережах, та протестувати різні методи їх вирішення.

Основний процес побудови користувацької мережі на базі ONOS кластеру включає кілька етапів, що відображені на рис. 1.

```
#!/usr/bin/python

from mininet.topo import Topo
from mininet.net import Mininet
from mininet.link import TCIntf
from mininet.link import TCLink
from mininet.node import Controller, OVSSwitch, RemoteController
from mininet.cli import CLI
from mininet.log import setLogLevel

def multiControllerNet():
#    Create a network from semi-scratch with multiple controllers

    net = Mininet( controller=Controller, switch=OVSSwitch, link=TCLink )

    print '*** Creating switches'
    s1 = net.addSwitch( 's1' )
    s2 = net.addSwitch( 's2' )
    s3 = net.addSwitch( 's3' )
    s4 = net.addSwitch( 's4' )


    print '*** Creating hosts'
    h1 = net.addHost( 'h1' )
    h2 = net.addHost( 'h2' )
    h3 = net.addHost( 'h3' )
    h4 = net.addHost( 'h4' )


    print '*** Creating links'
    net.addLink( s1, s2 )
    net.addLink( s1, s3 )
    net.addLink( s2, s3 )
    net.addLink( s2, s4 )
    net.addLink( s3, s4 )
    net.addLink( s1, h1 )
    net.addLink( s2, h2 )
    net.addLink( s3, h3 )
    net.addLink( s4, h4 )


    print '*** Creating (reference) controllers'
    c1 = RemoteController( 'c1', ip='172.17.0.5', port=6653 )
    c2 = RemoteController( 'c2', ip='172.17.0.6', port=6653 )
    c3 = RemoteController( 'c3', ip='172.17.0.7', port=6653 )


    print '*** Starting network'
    net.start()
    c1.start()
    c2.start()
    c3.start()

    s1.start( [ c1, c2, c3 ] )
    s2.start( [ c1, c2, c3 ] )
    s3.start( [ c1, c2, c3 ] )
    s4.start( [ c1, c2, c3 ] )


    print '*** Running CLI'
    CLI( net )

if __name__ == '__main__':
    setLogLevel( 'info' )  # for CLI output
    multiControllerNet()
```

Рис.2. Опис мережевої топології на API Mininet у вигляді python-файлу.

Етап 1. Починаючи з розгортання контролерів ONOS, першим кроком є встановлення необхідного програмного забезпечення на вузлах кластеру, на яких будуть працювати контролери. Для цього знадобиться комп’ютер із не менше 8 ГБ оперативної пам’яті та не менше 20 ГБ вільного місця на жорсткому диску. Швидший процесор або твердотільний накопичувач пришвидшить час завантаження віртуальної машини. Комп’ютер може працювати під керуванням Windows, Mac OS X або Linux – усі добре працюють із VirtualBox, єдиною програмною вимогою.

Запуск кластера зазвичай відбувається за допомогою інструментів контейнеризації, таких як Docker або Kubernetes. Кожен контролер

запускається як окремий контейнер, і всі контейнери підключаються до мережі, якою вони керують. Зв'язок між віртуальною машиною та контейнерами здійснюється через мережеву взаємодію. Запуск кластеру в нашому випадку виконується за допомогою скрипта, котрий під час запуску звертається до Docker Hub та завантажує контейнери контролерів на нашу віртуальну машину, компілює їх і запускає.

Етап 2. Після встановлення контролерів, необхідно створити віртуальну користувацьку мережу (див. рис. 3), а саме новий файл топології (див. рис. 2) користувацької мережі Mininet з розширенням ".py", наприклад: «topo.py». У якому слід визначити топологію мережі за допомогою API Mininet, вказавши кількість хостів, комутаторів, налаштувавши зв'язки між елементами мережі, а також прописати порядок запуску компонентів мережі. Далі потрібно визначити контролер ONOS, до якого потрібно підключитися, використовуючи також API. Запуск написаної топології, можна виконати шляхом виконання, у терміналі віртуальної машини, команди:

```
>> sudo python topo.py
```

Наповнення файлу «topo.py» виглядає наступним чином:

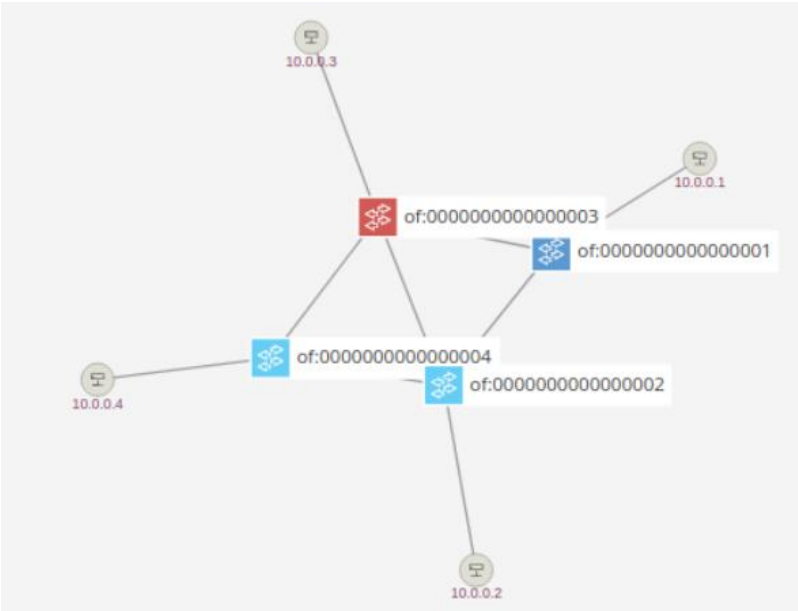


Рис.3. Користувацька топологія та підпорядковування комутаторів різним контролерам в кластері.

Етап 3. Після виконання команди вище, кожен контролер ONOS підключається до мережі і отримує інформацію про стан мережі та мережевий трафік. Інформація обмінюється між контролерами за допомогою протоколу OpenFlow або NETCONF. Таким чином, контролери працюють як розподілені системи, що спільно керують мережею і забезпечують її ефективну роботу.

Етап 4. Після створення мережі, необхідно виконати налаштувати мережевих сервісів та трафіку в ONOS. Для цього можна використовувати графічний інтерфейс або API, який дозволяє отримувати доступ до

різноманітних функцій та сервісів. Наприклад, за допомогою API можна налаштовувати правила маршрутизації, керувати розподіленням навантаження на вузлах мережі, налаштовувати мережеві сервіси тощо.

Графічний інтерфейс ONOS надає можливість керувати різними мережевими додатками, які можуть бути використані для управління мережею та її ресурсами. Основні мережеві додатки, які можна вмикати за допомогою графічного інтерфейсу ONOS, описані нижче:

- Host Location: цей додаток дозволяє відстежувати місцезнаходження хостів у мережі та контролювати їх рух.
- Intent: цей додаток використовується для створення та керування цілями (intents), які можуть бути використані для налаштування мережі та ресурсів.
- Link Connectivity: цей додаток дозволяє відстежувати зв'язок між різними вузлами у мережі та забезпечує стійкість мережі.
- OpenFlow: цей додаток використовується для встановлення зв'язку між контролером та OpenFlow-сумісними комутаторами.

Узагальнюючи результати роботи, було описано побудову користувацької мережі на базі ONOS кластеру з залученням платформи емуляції SDN Mininet. Було розглянуто процес побудови кластеру ONOS, системні вимоги та варіант розгортання на Linux. Було відображено процес описання топології віртуальної мережі за допомогою мови python на одному з рівнів Mininet API, підключення мережі до віддаленого контролера. Описані мережеві сервіси, що можна вмикати через графічний інтерфейс контролера та API. Також було наведено можливі проблеми, які можна вирішити за допомогою побудови мережі на базі ONOS та Mininet.

Література

1. Bhargavi Goswami. Experimenting with ONOS Scalability on Software Defined Network, January 2019, Journal of Advanced Research in Dynamical and Control Systems, ISBN: 1943-023X.
2. James Akerele. PERFORMANCE ANALYSIS OF OPENFLOW-ENABLED NETWORK TOPOLOGIES: OPENFLOW SDN VS TRADITIONAL NETWORK, January 2018, DOI:10.13140/RG.2.2.33523.84008.
3. Luca Boero, M. Cello, Mario Marchese, C. Garibotto. BeaQoS: Load balancing and deadline management of queues in an OpenFlow SDN switch, September 16, ISBN: 1389-1286.
4. Oleksandr Ivanovich Romanov, Ivan Saychenko, Anton Marinov, Serhii Skolets. RESEARCH OF SDN NETWORK PERFORMANCE PARAMETERS USING MININET NETWORK EMULATOR, June 2021, Information and Telecommunication Sciences, DOI:10.20535/2411-2976.12021.24-32.
5. Romanov, O., Korniienko, N., Burlaka, H. Construction of the SDN Transport Network Model using the T-API Interface/2021 IEEE 4th International Conference on Advanced Information and Communication Technologies, AICT 2021 - Proceedings, 2021, стр. 220–224.
6. Romanov, O., Siemens, E., Nesterenko, M., Mankivskyi, V. Mathematical description of control problems in SDN networks/Proceedings of International Conference on Applied Innovation in IT, 2021, 9(1), стр. 33–39.

УДК 621.391

ОСОБЛИВОСТІ ПОБУДОВИ РОЗПОДІЛЕНОЇ МЕРЕЖЕВОЇ ОПЕРАЦІЙНОЇ СИСТЕМИ ONOS

Нестеренко М.М., Сколець С.С., Марінов А.І.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: nikolaiy.nesterenko@gmail.com, *serskols@gmail.com, anton_marinov@ukr.net*

FEATURES OF THE CONSTRUCTION DISTRIBUTED NETWORK OPERATING SYSTEM ONOS

This article discusses the ONOS distributed network operating system, which provides a software-defined approach to network management, enabling a more flexible and efficient approach to managing network resources. Key features of ONOS are analyzed, such as traffic management, event processing, monitoring and analysis of network data, network topology construction, and management of network services.

У статті розглянуто розподілену мережеву операційну систему ONOS, що надає можливість програмного керування мережею, що забезпечує більш гнучкий та ефективний підхід до керування мережевими ресурсами. Проаналізовані ключові можливості ONOS, такі як: керування трафіком, обробка подій, моніторинг та аналіз мережевих даних, побудова мережевих топологій, управління мережевими сервісами.

На сьогодні мережеві інфраструктури зазвичай стикаються з проблемою обмеженості традиційних мережевих архітектур, які працюють на основі жорстко заданих правил і не забезпечують достатньої гнучкості та ефективності управління мережею. Це створює серйозні обмеження для розробників і операторів мереж, які потребують змін та ефективного підходу до керування мережевими ресурсами.

Крім того, існуючі мережеві архітектури не забезпечують достатньої масштабованості та гнучкості для відповіді на зростаючі вимоги до обслуговування мережі, такі як забезпечення високої доступності, масштабування та обробка великого обсягу трафіку. Тому була необхідність у створенні нової мережевої архітектури, яка б забезпечувала більш оптимальний підхід до керування мережевими ресурсами. І саме відкрите програмне забезпечення ONOS створено для вирішення цих проблем на основі підходу SDN.

ONOS включає в себе контролер SDN, який дозволяє віддалено керувати трафіком мережі, забезпечувати балансування навантаження, реалізовувати механізми безпеки мережі та інші функції, які раніше були залежні від вбудованих протоколів комутації.

ONOS також забезпечує відкритий API для взаємодії з різними програмами та системами, що дозволяє використовувати його в різних

середовищах та інтегрувати з різними компонентами мережі. Додатково, ONOS має розширювану архітектуру, яка дозволяє розробникам створювати свої власні модулі та додатки для розширення функціональності системи.

ONOS має модульну архітектуру, яка зображена на рис.1.

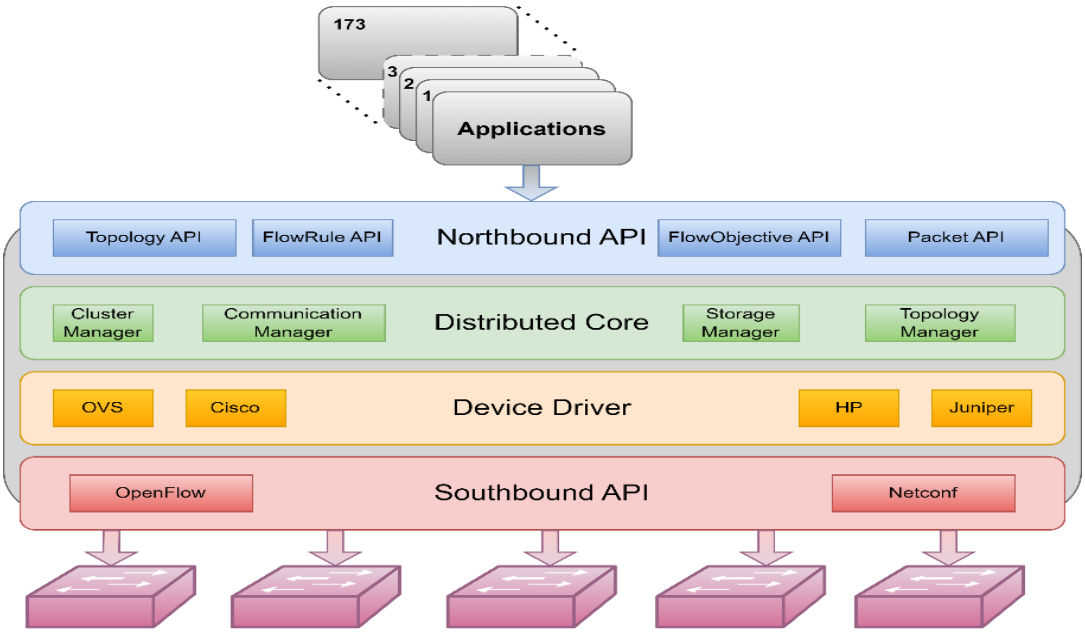


Рис.1. Архітектура побудови кластеру ONOS.

Рівень 1. Applications – Додатки – це верхній рівень архітектури ONOS, який представляє собою множину додатків, що реалізовані на основі платформи ONOS. Кожен додаток може мати власну логіку та функціональність, такі як керування трафіком, моніторинг мережевих подій, керування сервісами тощо.

Рівень 2. Northbound API – Північні API – це рівень, який забезпечує доступ до функцій ONOS через стандартні інтерфейси API, які можуть використовуватися додатками, контролерами та іншими системами. Цей рівень дозволяє розробникам додатків легко інтегрувати їх з платформою ONOS та взаємодіяти з нею.

Рівень 3. Distributed core – Розподільне ядро – це рівень, який забезпечує роботу платформи в розподіленому середовищі. ONOS може працювати на декількох вузлах, і цей рівень дозволяє розподіляти завдання між різними вузлами та координувати їхню роботу. На цьому рівні міститься основна логіка системи, яка складається з декількох компонентів, таких як:

- Cluster Manager: відповідає за управління розподіленим середовищем. Він забезпечує обмін інформацією між контролерами і зберігання даних.
- Communication Manager: забезпечує зв'язок між різними контролерами ONOS.

- Storage Manager: забезпечує зберігання інформації про стан мережі, налаштування та інші дані, які потрібні для роботи контролерів.
- Topology Manager: відповідає за збір інформації про топологію мережі і побудову топологічного зображення для аналізу та керування мережею.

Рівень 4. Device driver – Драйвера пристрою – це рівень, який забезпечує взаємодію з мережевими пристроями, такими як комутатори або маршрутизатори. Кожен пристрій мережі потребує власного драйвера, який забезпечує комунікацію.

Рівень 5. Southbound API – Південні API – це інтерфейс між ONOS і сумісними з ним мережевими елементами. Цей рівень архітектури відповідає за взаємодію з різними мережевими пристроями, такими як комутатори, маршрутизатори та інші. Підтримуються різні протоколи, такі як OpenFlow, NETCONF та OVSDB, щоб забезпечити взаємодію з різними мережевими елементами.

Рівень 6. Data plane – Площина данних – це частина мережі, що відповідає за передачу даних. У даному випадку, вона складається з комутаторів, маршрутизаторів та інших мережевих пристроїв. ONOS взаємодіє з data plane через southbound API, щоб забезпечити керування мережею.

Насправді, найцікавішим та важливим у роботі контролера є рівень додатків, оскільки саме вони додають нові можливості або змінюють поведінку контролера, а отже мережі в цілому. Додатки реалізовані як окремі модулі, які можна встановлювати, оновлювати, видаляти і запускати з інтерфейсу ONOS. Рівень додатків також забезпечує можливість взаємодії додатків між собою та з іншими рівнями контролера.

Додатки можуть включати у себе різноманітні функції, такі як підтримка різних протоколів мережі, управління ресурсами мережі, маршрутизація, збір даних, аналіз мережі та багато іншого. Рівень додатків дозволяє розширити функціональність контролера ONOS та адаптувати його до конкретних потреб мережі. Кількість додатків, що автоматично вмикаються при запуску контролера ONOS, залежить від конфігурації та налаштувань системи. Зазвичай за замовчуванням вмикаються деякі базові додатки, необхідні для правильної роботи контролера ONOS.

Деякі з базових додатків, автоматично вмикаються при запуску ONOS, та включають:

OpenFlow Provider Suite (OF) - додаток для підтримки протоколу OpenFlow.

Link Layer Discovery Protocol (LLDP) - додаток для виявлення інформації про з'єднання мережевих пристроїв.

Network Configuration Protocol (Netcfg) - додаток для налаштування мережевих параметрів.

Open Virtual Network (OVN) - додаток для підтримки віртуальних мереж.

Intent Framework (INT) - додаток для виконання інтентів (намірів) у мережі.

Reactive Forwarding (Reactive) - додаток для реактивної маршрутизації пакетів в мережі.

Загальна кількість додатків, які можуть автоматично вмикатись при запуску ONOS, може варіюватись в залежності від версії ONOS, конфігурації та налаштувань системи, зазвичай це мінімум 173 додатки.

Узагальнюючи вище описане можна зробити висновок, що побудова мереж SDN на базі контролеру ONOS дозволяє побудувати більш гнучку та ефективну мережу, що може бути пристосована до конкретних потреб користувачів. Крім того, ONOS забезпечує швидку реакцію на зміни в мережі та високу продуктивність, що є важливими факторами для багатьох організацій. Також у ході виконання роботи було проаналізовано особливості архітектури ONOS та її складових, такі як рівні додатків, рівень керування топологією мережі, рівень обробки потоків даних та рівень інфраструктури .

Література

1. Diego Kreutz, Fernando M. V. Ramos, Paulo Veríssimo, Christian Esteve Rothenberg. Software-Defined Networking: A Comprehensive Survey, June 2014, Proceedings of the IEEE. DOI:10.1109/JPROC.2014.2371999
2. Romanov, O., Nesterenko, M., Mankivskyi, V., Zhuk, O. Principles of Building Modular Control Plane in Software-Defined Network//Lecture Notes in Networks and Systems, 2023, 548, pp. 333–355, DOI: 10.1007/978-3-031-16368-5_17

https://link.springer.com/chapter/10.1007/978-3-031-16368-5_17

3. Pedro Sousa, Gonçalo Pereira, Jose Silva. Comparative Study of Software-Defined Networking (SDN) Traffic Controllers, Jun 2019, 2019 14th Iberian Conference on Information Systems and Technologies (CISTI),DOI: 10.23919/CISTI.2019.8760997
4. Romanov, O., Korniienko N., Svyd I., Romanov A. Optical Network Management by ONOS-Based SDN Controller, September 2022, Radiotekhnika, DOI:10.30837/rt.2022.3.210.16
5. Edson Tavares de Camargo, Rogério C. Turchetti, Lucas V. Ruchel. Evaluation of the robustness of SDN controllers ONOS and ODL, Oct 2022, DOI:10.1016/j.comnet.2022.109403
6. Документація ONOS: https://wiki.onosproject.org/display/ONOS/Documentation

УДК 004.738

МОДЕЛЮВАННЯ МЕРЕЖІ SDN НА СТОРОНІ КІНЦЕВОГО КОРИСТУВАЧА

Сайченко І.О.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: paramayson@gmail.com

SDN NETWORK SIMULATION ON THE END-USER SIDE

End-user SDN modeling is the process of creating a virtual SDN network on a local computer for network testing and analysis. This process provides an opportunity to determine the optimal parameters of the network and to investigate its operation in different conditions.

Software Defined Networking (SDN) – це нова технологія мережевого управління, яка надає більш гнучкий та простіший підхід до управління мережами, зменшуючи складність і покращуючи ефективність. У традиційних мережах, управління мережевими пристроями відбувається з точки зору апаратного забезпечення. SDN використовує програмне забезпечення для забезпечення контролю і керування мережею, що робить його більш гнучким та ефективним. SDN мережі дозволяють розподіляти пропускну здатність на основі потреб користувачів і управляти мережевим трафіком в режимі [1].

Основні концепції SDN. SDN – як архітектура мережі дозволяє розподіляти мережеву пропускну здатність на основі потреб користувачів. Основний принцип SDN полягає у розділенні мережевого контролю та пересилання даних на окремі пристрої. Мережевий контроль виконується на центральному контролері, який керує всіма мережевими пристроями, тоді як пересилання даних відбувається на комутаторах.

Одним з основних елементів SDN є контролер (рис. 1), який відповідає за керуванням мережевими пристроями. Контролер може бути фізичним або віртуальним, залежно від конфігурації мережі. Він приймає рішення про розподіл пропускної здатності, на основі потреб користувачів та стану мережі. Контролер використовує протокол OpenFlow для взаємодії з комутаторами та іншими мережевими пристроями [2].

Комутатори в SDN мережах мають більш просту архітектуру порівняно з традиційними комутаторами. Вони не мають вбудованого розподілу пропускної здатності та правил маршрутизації. Комутатори виконують інструкції, які отримують від контролера через протокол OpenFlow.

Моделювання мережі SDN на стороні кінцевого користувача. Моделювання мережі SDN на стороні кінцевого користувача – це процес створення віртуальної SDN мережі на локальному комп'ютері, для тестування та аналізу мережі. Цей процес забезпечує можливість визначити оптимальні параметри мережі та дослідити її роботу в різних умовах.

Для моделювання мережі SDN на стороні кінцевого користувача використовуються віртуальні середовища, такі як Mininet [3], GNS3 [4] та інші.

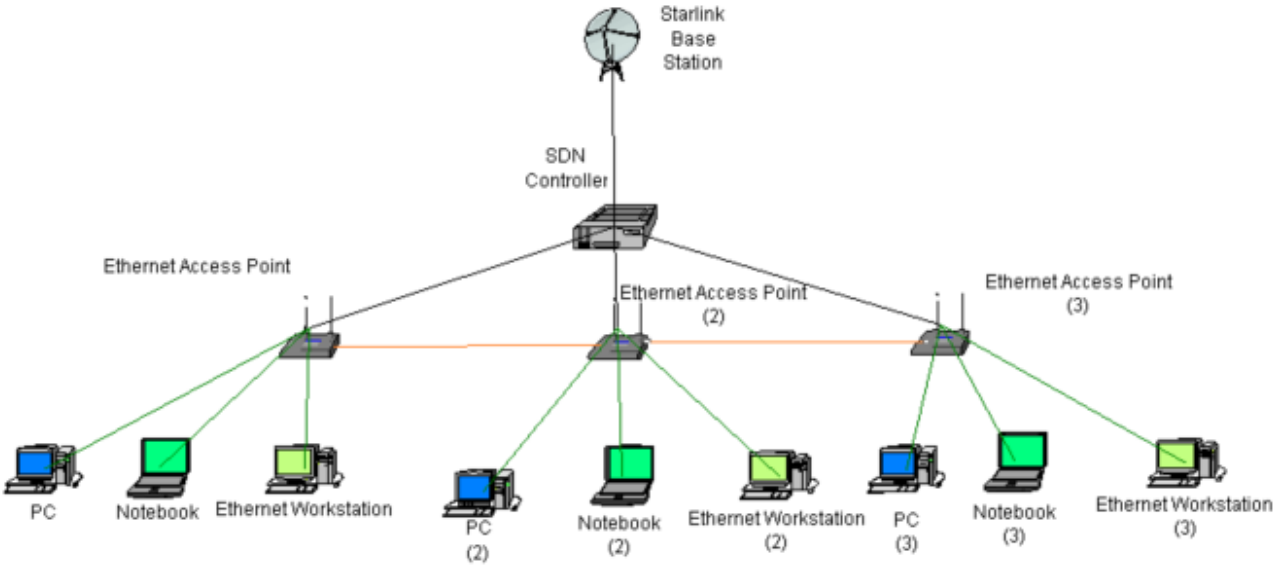


Рисунок 1. Модель мережі SDN з кінцевими користувачами та супутнім обладнанням.

Ці середовища дозволяють створити віртуальну мережу з декількох віртуальних комутаторів, хостів та контролерів, що дозволяє досліджувати роботу мережі та тестувати її функціональність [5].

Процес моделювання мережі SDN на стороні кінцевого користувача включає наступні етапи:

1. Встановлення віртуального середовища: для створення віртуальної мережі необхідно встановити віртуальне середовище, таке як Mininet або GNS3. Ці середовища дозволяють створити віртуальну мережу на локальному комп'ютері.

2. Створення топології мережі: після встановлення віртуального середовища необхідно створити топологію мережі, яка включає в себе віртуальні комутатори, хости та контролери.

3. Налаштування параметрів мережі: після створення топології мережі необхідно налаштувати параметри мережі, такі як розмір буфера, пропускну здатність та правила маршрутизації.

4. Тестування мережі: після налаштування параметрів мережі можна почати тестування мережі, щоб перевірити її функціональність та виявити проблеми.

5. Аналіз результатів: після завершення тестування мережі необхідно проаналізувати результати тестування та визначити оптимальні параметри мережі.

Graphical Network Simulator, це графічний емулятор мережі, який дозволяє створювати різні мережеві топології безпосередньо на комп'ютері. GNS3 зазвичай використовується як лабораторний майданчик для перевірки технологій та схем. Однак, GNS3 - це емулятор, а не симулятор, і варто розуміти різницю між цими термінами для користувача. Емулятор дозволяє

створити модель комп'ютера або пристрою та запустити в ньому оригінальне програмне забезпечення, емулюючи всі основні компоненти пристрою, включаючи процесор, пам'ять та пристрої введення/виведення. В разі емуляції пристроїв Cisco [6], створюється модель маршрутизатора яка запускає в ньому реальну операційну систему Cisco IOS, що дозволяє отримати повнофункціональний маршрутизатор.

З іншого боку, симулятор імітує поведінку системи та її інтерфейсу, наприклад, Cisco Packet Tracer створює пристрої зі схожим інтерфейсом та командами.

Переваги використання GNS3:

1. Перша та головна перевага полягає в повному функціоналі емульованих пристроїв. Це означає, що при запуску маршрутизатора Cisco у GNS3, користувач має доступ до практично всіх функцій, які працюють на реальному маршрутизаторі. У порівнянні з Cisco Packet Tracer, де значна частина функціоналу є недоступною через його симулюючий характер.

2. Можливість побудови гетерогенних мереж. За допомогою GNS3 користувач може створити мережу, де присутні не лише пристрої Cisco, але й Juniper, Mikrotik, CheckPoint тощо. Це моделює реальне життя, де мережа зазвичай складається з обладнання різних виробників.

3. У GNS3 можна додавати повноцінні робочі станції та сервери, що відрізняє його від Cisco Packet Tracer, де клієнтські комп'ютери або сервери мають обмежені можливості. З використанням технологій віртуалізації (як приклад VirtualBox або VMWare) або підключенням до реально існуючої розгорнутої мережі, користувач може додати комп'ютери з операційними системами, такими як Windows або Ubuntu, а також сервери, такі як Windows Server чи RedHat. Це дає змогу перевірити роботу різних функціональних можливостей, таких як встановлення VPN клієнта на робочу станцію, автентифікація користувачів через сервер AAA, а також використання браузера при підключенні до Інтернету. Все це дозволяє наблизити умови тестових лабораторних досліджень до реальних умов розгортання, навантаження та використання.

4. Безкоштовність є ще однією важливою перевагою GNS3. ПЗ доступний для використання без будь-яких обмежень, що робить його особливо привабливим. На відміну від Cisco Packet Tracer, який може бути незаконно завантажений, GNS3 є безкоштовним і доступним для всіх користувачів. І хоча є інші платні симулятори та емулятори, такі як Boson NetSim або Cisco VIRL, GNS3 залишається безкоштовним та доступним для всіх.

Недоліки використання GNS3

1. Головний недолік полягає в тому, що GNS3 не може емулювати комутатори через використання великої кількості ASIC мікросхем, які неможливо емулювати на звичайному комп'ютері. Ці мікросхеми забезпечують велику швидкість обробки пакетів, тоді як маршрутизатори працюють на процесорі, що значно повільніший за ASIC мікросхеми. Однак, на практиці проблем із емуляцією маршрутизатора не виникає.

2. Значний недолік полягає в високих вимогах до системних ресурсів. GNS3 працює з реальними ПЗ пристроїв, що вимагає значно більше ресурсів, ніж симуляції у Cisco Packet Tracer. Наприклад, запуск Cisco ASA вимагає 1 Гб оперативної пам'яті, а збирання кластера або включення Cisco IPS може додати ще 1 Гб. Мінімальні системні вимоги для GNS3 сьогодні становлять 4 Гб оперативної пам'яті, але рекомендується мати хоча б 8 Гб для складних схем та зручності обчислень.

3. Третій недолік полягає в наявності програмних помилок. GNS3 має чимало помилок, які виправляються в нових версіях, але кожен реліз нової версії може також мати нові помилки. Це може бути незручно для користувачів, але важливо навчитися користуватися інструментом незалежно від цих помилок.

Моделювання мережі SDN на стороні кінцевого користувача виступає корисним для розробників мережевих додатків, мережевих інженерів та адміністраторів мережі. Цей процес дозволяє тестувати різні параметри мережі та виявляти проблеми до їх виникнення у реальній мережі. При роботі з мережами та їх моделюванням (особливо з обладнанням Cisco), знання GNS3 перетворюються в необхідний інструмент на ряду з апаратним обладнанням. Це ПЗ являє собою практично повноцінний лабораторний стенд, де можна макетувати потрібні схеми чи рішення, перевірити конфігурацію перед застосуванням на реальному пристрої. І вся ця лабораторія розгорнута в одному комп'ютері. Це суттєво заощадить як кошти так і час на підготовку та впровадження програмно конфігурованих рішень.

Література

1. Open Networking Foundation. (2021). "SDN Architecture Overview" [Онлайн]. Доступно: https://www.opennetworking.org/sdn-resources/sdn-definition/ [Доступ: 13 березня 2023 р.].
2. Open Networking Foundation. (2021). "OpenFlow Switch Specification." [Онлайн]. Доступно: https://www.opennetworking.org/wp-content/uploads/2014/10/openflow-switch-v1.4.0.pdf [Доступ: 13 березня 2023 р.].
3. Mininet. (2018). "Mininet Documentation." [Онлайн]. Доступно: http://mininet.org/documentation/ [Доступ: 13 березня 2023 р.].
4. GNS3. (2021). "GNS3 Documentation." [Онлайн]. Доступно: https://docs.gns3.com/ [Доступ: 13 березня 2023 р.].
5. D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, S. Uhlig. "Software-Defined Networking: A Comprehensive Survey". Proceedings of the IEEE. 2015.
6. Cisco. (2021). "Cisco Application Centric Infrastructure (ACI)." [Онлайн]. Доступно: https://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/index.html [Доступ: 13 березня 2023 р.].

УДК 621.39

АПАРАТНО-ПРОГРАМНИЙ КОМПЛЕКС ДЛЯ ДОСЛІДЖЕННЯ ПАРАМЕТРІВ СИГНАЛІВ СУПУТНИКОВОГО ТЕЛЕВІЗІЙНОГО МОВЛЕННЯ

Дрьомова А.О., Авдєєнко Г.Л.
Київська Мала академія наук учнівської молоді, Україна
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: angy.drom@gmail.com

HARDWARE AND SOFTWARE COMPLEX FOR RESEARCHING THE PARAMETERS OF SATELLITE TELEVISION BROADCASTING SIGNALS

Dromova A.O., Avdeenko G.L.
Kyiv Junior Academy of Sciences of Student's Youth, Ukraine
Educational and Scientific Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

The article describes the development of a complex for the study of satellite television broadcasting signals using a combined hardware and software method. The laboratory testing of the created development was carried out, and the hypothesis of combining hardware and software methods for measuring the parameters of satellite television broadcasting signals was confirmed.

Телевізійне мовлення досі зберігає свою популярність. Перед користувачами та розробниками систем супутникового телебачення постає проблема покращення якості приймання супутникового сигналу. Супутникове телевізійне мовлення здійснюється у ділянці Ku-діапазону (10,7...12,75 ГГц), яка є найпопулярнішою та найбільш використовуваною.

У 1994 р. було розроблено стандарт супутникової цифрової системи багатопрограмного телевізійного мовлення DVB-S. Робоча смуга частот для систем даного стандарту займає Ku-діапазон (10,7...12,75 ГГц). Стандарт супутникової цифрової системи DVB-S2 — специфікація другого покоління, розроблена на основі специфікації першого покоління DVB-S для передавання більшого обсягу корисної інформації в заданій смузі частот з мінімальними витратами на приймальній частині системи.

Дослідження параметрів сигналів супутникового телевізійного мовлення здійснюються регулярно з метою підвищення ефективності роботи його систем. До основних параметрів сигналів супутникового телебачення належать потужність, частота, поляризація електромагнітної хвилі, модуляція, ширина спектра, відношення сигнал/шум, імовірність бітової помилки, символьна швидкість. Для кількісної оцінки параметрів сигналів

супутникового телевізійного мовлення використовується спеціалізована вимірювальна техніка (аналізатори сигналу, спектру) і програмне забезпечення.

Було висунуто гіпотезу: шляхом комбінування апаратних та програмних елементів можливо забезпечити оптимальну точність вимірювань параметрів сигналів супутникового телевізійного мовлення. У створеному комплексі застосовується комбінований метод вимірювання параметрів сигналів супутникового телевізійного мовлення.

Метою статті є підтвердження гіпотези про забезпечення максимальної точності вимірювань параметрів сигналів супутникового телевізійного мовлення шляхом комбінування апаратного та програмного методів.

Для підтвердження висунутої гіпотези було виконано наступні завдання:

1) досліджено теоретичні основи функціонування систем супутникового телевізійного мовлення та методів вимірювання параметрів сигналів супутникового телевізійного мовлення;

2) здійснено комп'ютерне моделювання системи супутникового телевізійного мовлення стандартів DVB-S, DVB-S2 для дослідження особливостей приймання сигналу (див. рис. 1);

3) створено макетний зразок апаратно-програмного комплексу для дослідження параметрів сигналів супутникового телевізійного мовлення;

4) здійснено лабораторну апробацію створеної розробки для перевірки її функціональності.

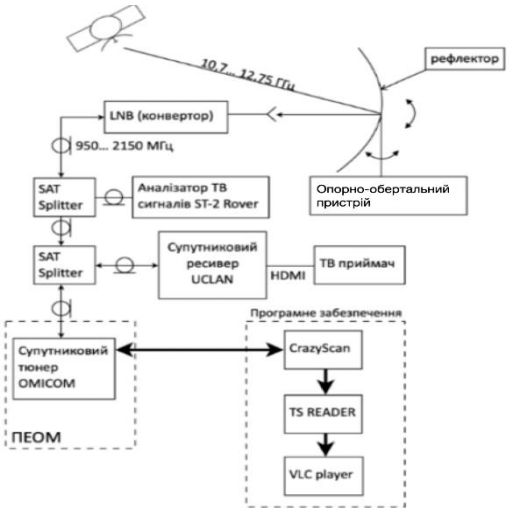


Рис. 1. Схема створеного комплексу.

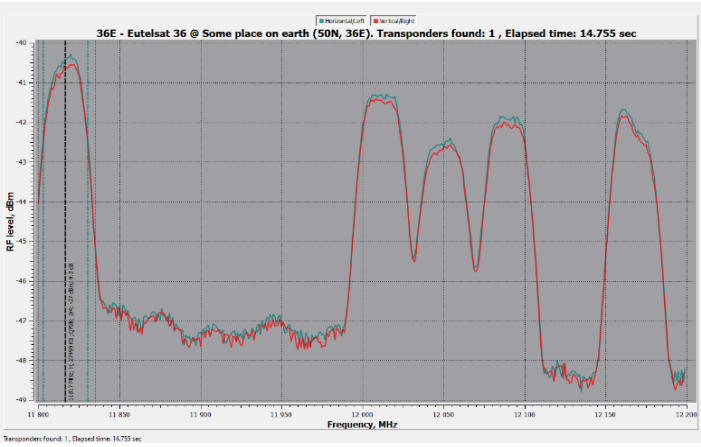


Рис. 2. Візуалізація спектрів прийнятих сигналів програмним забезпеченням CrazyScan.

Лабораторна апробація створеної розробки полягала у прийманні сигналу з обраного супутника та дослідженні його параметрів. За допомогою даного комплексу було досліджено параметри сигналів супутників з сузір'я

Astra (Astra 5B, Astra 2E, Astra 2G, Astra 2F). За результатами лабораторної апробації було підтверджено: функціональність створеного апаратно-програмного комплексу; гіпотезу про комбінування методів вимірювання параметрів сигналу супутникового телевізійного мовлення (див. Таблицю 1).

Таблиця 1. Порівняння переваг і недоліків апаратного, програмного та комбінованого методів вимірювання параметрів сигналу.

	Апаратний метод	Програмний метод	Комбінований метод
Отримання даних у режимі реального часу	+	-	+
Детальне дослідження, аналіз параметрів сигналу	-	+	+
Визначення частоти транспондера, типу модуляційного сузір'я	-	+	+
Візуалізація діаграми сигнального сузір'я та спектру сигналу	-	+	+

Висновки. Результати лабораторної апробації підтвердили гіпотезу про комбінування методів дослідження сигналу; лабораторна апробація підтвердила можливість практичного використання розробки для моніторингу стану систем супутникового ТВ мовлення.

Література

1. Бадялик В.П. Основы телевизионного вещания со спутников. Москва: Горячая линия–Телеком, 2004. 39-40 с.
2. Данилин А. А. Спутниковое телевидение. Установка, подключение, ремонт. Москва: СОЛОН-ПРЕСС, 2009. 36-37 с.
3. Мамаев Н. С., Мамаев Ю. Н., Теряев Б. Г. Системы цифрового телевидения и радиовещания. Москва: Горячая линия–Телеком, 2007. 124-133 с.
4. Методичні рекомендації до виконання лабораторних робіт з дисципліни «Технології радіо- та телевізійного мовлення» для студентів спеціальності 172 «Телекомунікації та радіотехніка» спеціалізацій «Апаратно-програмні засоби електронних комунікацій», «Мобільні телекомунікації». Київ: Міністерство освіти і науки України, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Інститут телекомунікаційних систем, 2019. 9-18 с.
5. Benoit H. Digital television: Satellite, Cable, Terrestrial, IPTV, Mobile TV in the DVB Framework. Waltham: Focal Press, 2008. 119 с.
6. Eastment J., Otung I., Uggala L. Mitigating the effects of rain-induced fading in satellite systems using Time Diversity in concert with Maximal Ratio Combining. The Journal of Engineering. 2016. Вип. 6. 10 с.
7. Fischer W. Digital Video and Audio Broadcasting Technology: A Practical Engineering Guide (Signals and Communication Technology). New York: Springer, 2020. 240-264 с.

УДК 621.395

ПОБУДОВА МЕРЕЖІ ШИРОКОСМУГОВОГО ДОСТУПУ З ПІДТРИМКОЮ SDN НА БАЗІ ПЛАТФОРМИ SEBA

[1]Поливана В.В., [2]Романов М. О.
[1]*Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна*
[2]*Національний авіаційній університет, Київ*
E-mail: viky77710@gmail.com, goraciu@gmail.com

CONSTRUCTION A BROADBAND ACCESS NETWORK WITH SDN SUPPORT BASED ON THE SEBA PLATFORM

SDN Enabled Broadband Access (SEBA) is a large open source development and integration project organized by the Open Network Foundation (ONF). SEBA is a designed to support the network and functional needs of several operators with a general architecture. SEBA's reference design (RD) provides a high-level template or architecture to support broadband with minimal purpose technological choice.

У сучасному світі мережі потребують більш високої швидкості передачі даних і поліпшення інструментів, що використовуються для управління мережами та моніторингом. Ці обставини призвели до появи нових функціональних і технологічних мереж зі складними інфраструктурами, а саме виникнення нової концепції побудови мереж на основі SDN (Software-Defined Networking) архітектури. Крім цього сучасні тенденції розвитку інформаційних технологій чітко змінюють корпоративні мережі, постійно спостерігається збільшення обсягів мережевого трафіку, у зв'язку з цим, виникає потреба в конфігурації постійного додавання складних мережних структур. Саме платформа SEBA надає можливість удосконалити мережі доступу по всьому світу для відкритих, керованих програмних забезпечень систем у нових ключових областях, бо якраз SEBA створена для надання шаблону архітектури для розробки рішень носіїв широкосмугового доступу [1].

SEBA – це платформа з відкритим вихідним кодом, яка віртуалізує широкосмугові мережі. Видобуваючи та «хмаруючи» більшість функцій, які традиційно виконувалися в складних PON-системах на базі шасі, оператори можуть використовувати системи PON (Passive Optical Network – система пасивної оптичної мережі складається з оптичного лінійного терміналу (OLT – Optical Line Terminal), який з'єднує кілька оптичних мережевих терміналів (ONT – Optical Network Terminal) за допомогою пасивної оптичної розподільчої мережі) від різних постачальників, використовуючи при цьому спільне програмне забезпечення для управління. Це оптимізує капітальні та операційні витрати, а також створює модель розгортання, яку прийняли провідні оператори.

Підхід дозволяє використовувати декілька потоків реалізації для відповідності SEBA вимог повністю або по частинах як сукупність модулів і

композицій, що дозволяють використовувати поєднання SDN, NFV (Network Function Virtualization), а також застарілі компонентів PNF (Physical Networking Function) для використання як композиційних елементів у розгортанні [2].

SEBA створена для надання шаблону архітектури для розробки рішень для широкосмугового доступу носіїв. Сфера застосування SEBA RD призначена для охоплення широкого набору бездротових і фіксованих технологій бездротового доступу і пов'язаних з ними можливостей Service Edge. До них відносяться, але не обмежуються: PON (Passive Optical Network), XGS-PON (10-Gigabit-capable Symmetric Passive Optical Network), NG-PON2 (Next-Generation Passive Optical Network 2), EPON (Ethernet Passive Optical Network), майбутні технології PON, Gfast, Ethernet, DOCSIS (Data Over Cable Service Interface Specification). Сфера застосування повинна дозволяти легко адаптувати нові технології, що підтримують ці технології та нові пристрої, які включають ці технології у елементи, що розгортаються. Це повинно бути можливо без переписування основних розділів підкомпонентів, з яких складається SEBA і не повинні вимагати нових фундаментальних взаємодій на північ від платформ автоматизації носіїв [1].

SEBA розроблений як набір контейнерних елементів, які працюють в середовищі Kubernetes. Система модульована на архітектуру типової мікросервісної системи та існує ієрархія модульності, яка використовується, щоб дозволяти гнучкі композиції в різних масштабах.

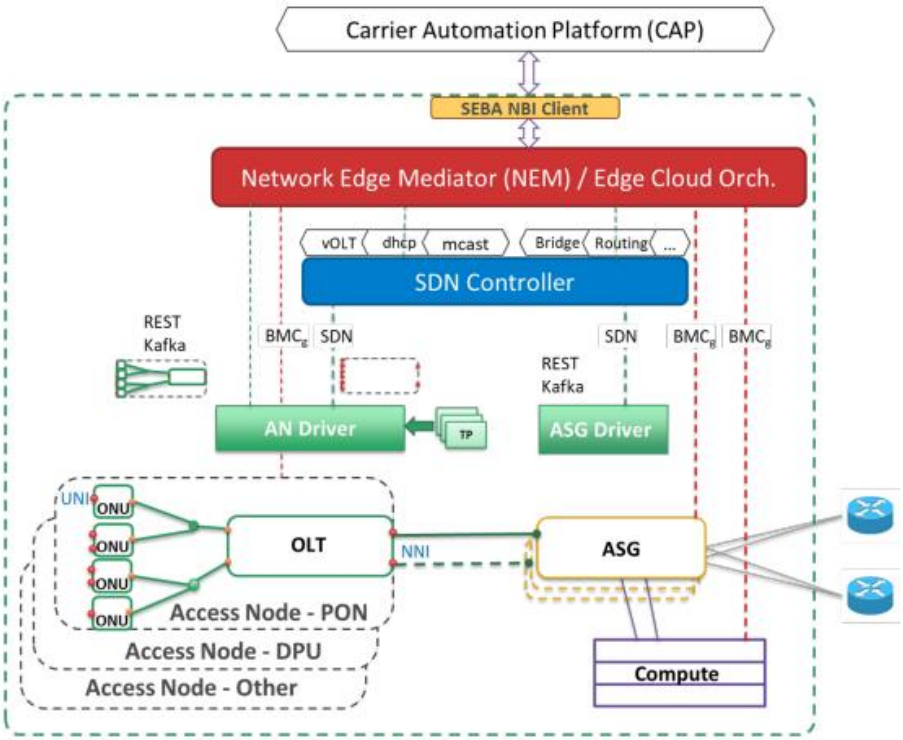


Рис.1. Попередня архітектура високого рівня SEBA.

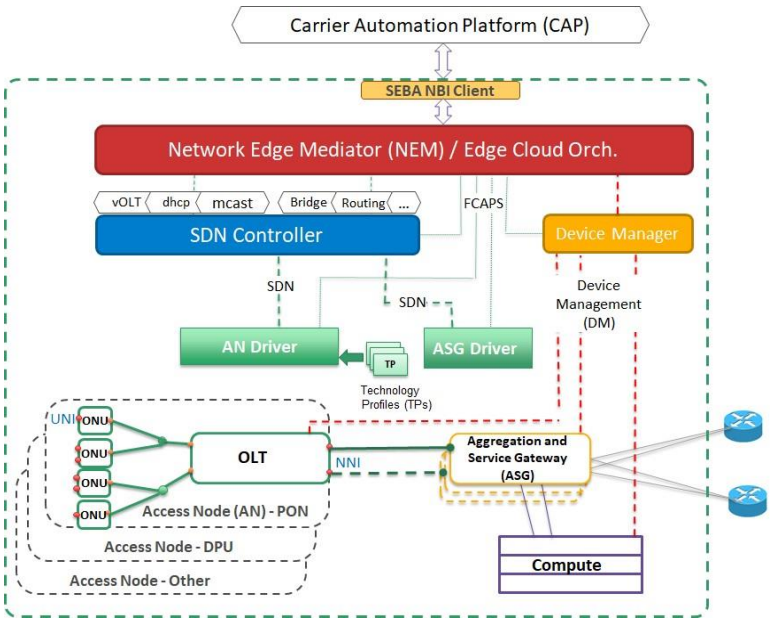


Рис. 2. Новітня модульна архітектура високого рівня SEBA.

На рис. 1 та рис. 2 показано, що SEBA складається з декількох програм модулів високого рівня, такі як:

- Модуль NEM - Network Edge Mediator;
- Модуль керування SDN;
- Модуль керування додатками;
- Драйвер доступу до вузла (AN);
- Драйвер агрегації та обслуговування (ASG);
- Диспетчер пристроїв.

Порівняно з попередньою моделлю (рис. 1) відбулися доповнення (рис.2), а саме:

- Детальні API-інтерфейси NBI для POD, OLT (Optical Line Terminal), ONT (Optical Network Terminal), управління сервісами;
- Оновлення широкосмугового мережевого шлюзу (BNG);
- Керування пристроями (DM);
- Модель стека OLT VOLTHA масштабування;
- Технологія доступу – фіксований бездротовий доступ (FWA) / mmWAVE.
- Варіанти використання для керування життєвим циклом POD [3].

Новітня архітектура вищого рівня стає більш корисною для розробників прикладів платформ, що змусить їх інтегруватися з системами експлуатаційної підтримки швидше ніж з операторами програмного забезпечення. Тому оновлення широкосмугового мережевого шлюзу дозволить підтримувати майбутні технології, а отже роботу через чітко визначені інтерфейси та моделі.

Тобто в API інтерфейсі, а саме управлінні POD визначаються такі компоненти: надання інформації про інвентаризацію, моніторинг апаратних ресурсів, звітність про стан, управління сигналізацією та моніторинг продуктивності.

В управлінні OLT (Optical Line Terminal) зазначається, що відбувається: постачання апаратним забезпеченням OLT, отримання списку пристроїв, отримання списку портів OLT NNI/PON, управління програмним забезпеченням та оновленнями OLT, запуск доступних діагностик OLT і отримання результатів, отримання інформації про інвентаризацію для SFP (Small Form-factor Pluggable) пристроїв та підключених до портів OLT.

В управлінні ONT відбувається: оновлення серійного номера обладнання ONT, отримання інформації про інвентаризацію обладнання ONT, управління програмним забезпеченням та оновленнями, управління асоційованими конфігураціями ONT DB, запуск доступної ONT діагностики та отримання результатів [3, 5].

SDN Широкосмуговий доступ (SEBA) є найуспішнішим дослідженням додатків SDN для мережі доступу, де кілька операторів рекламують комерційні розгортання. Отже, платформа SEBA працює швидко і дозволяє керувати різними технологіями віртуалізованого доступу інтегруючи з їх EMS вкінці мережі оператора. SEBA прагне керувати різними типами white-boxes OLT поширюючи запуск програмних модулів загального призначення серверів. Програмне забезпечення SEBA є відкритим вихідним кодом, що дозволяє різним операторам зв’язку та постачальникам, що вимагають реалізації кожної функції [4, 6].

Література

1. ONF SDN Enabled Broadband Access (SEBA) March 17, 2021 [reference design v2.0]. [Електронний ресурс] – Режим доступу до ресурсу: https://opennetworking.org/wp-content/uploads/2021/03/ONF-Reference-Design-SEBAv2.0FINAL3.pdf.
2. Das, S. From CORD to SDN Enabled Broadband Access (SEBA) [invited tutorial] December 4, 2020. Journal of Optical Communications and Networking. [Електронний ресурс] – Режим доступу до ресурсу: https://www.osapublishing.org/jocn/abstract.cfm?uri=jocn-13-1-A88.
3. Andrea Campanella (Moderator), Burak Gorkemli, Manuel Paul, Cemil Soylu, Mario Kind SEBA Techinar presentation, March 30, 2021. [Електронний ресурс] – Режим доступу до ресурсу: https://opennetworking.org/seba/
4. Takahiro Suzuki, Yushi Koyasako Member IEEE Demonstration of IEEE PON Abstraction for SDN Enabled Broadband Access (SEBA) – Journal of lightwave technology, October 15, 2021. [Електронний ресурс] - Режим доступу до ресурсу: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9512472
5. Oleksander Romanov; Mykola Nesterenko; Volodymyr Mankivskyi; Oleksandr Zhuk Principles of Building Modular Control Plane in Software-Defined Network, 2023,DOI: 10.1007/978-3-031-16368-5_17
6. Стаття: Романов О.І., Свид І.В., Корнієнко Н.І., Романов А.О. Управління оптичною мережею контролером SDN на базі ONOS//Радіотехніка, № 210, 2022, С.188-196, DOI:10.30837/rt.2022.3.210.16

UDC 621.396.946

ON ONE POSSIBILITY OF CONSTRUCTING BAND-PASS FILTERS BASED ON OPTICAL MICRO-RESONATORS WITH WHISPERING GALLERY OSCILLATIONS

Trubin A. A.
National Technical University of Ukraine "Kyiv Polytechnic Institute"
E-mail: atrubin9@gmail.com

ОДНА З МОЖЛИВОСТЕЙ ПОБУДОВИ СМУГОВИХ ФІЛЬТРІВ НА ОСНОВІ ОПТИЧНИХ МІКРОРЕЗОНАТОРІВ З КОЛИВАННЯМИ ШЕПОЧУЧОЇ ГАЛЕРЕЇ

Пропонується нове рішення задачі побудови смугових фільтрів за допомогою використання спеціальним чином оптимізованих режекторних структур, побудованих на оптичних микрорезонаторах з коливаннями шепочучої галереї. Показано, що за допомогою підбору параметрів зв'язку, розмірів та числа мікрорезонаторів, використовуючи періодичність резонансних частот коливань шепочучої галереї, можна реалізовувати різні смуги пропускання заданої ширини. Побудовано електродинамічні моделі режекторних фільтрів на мікрорезонаторах з коливаннями шепочучої галереї. Запропоновані фільтри можуть застосовуватись у пристроях DWDM оптоволоконних систем зв'язку.

Whispering gallery microresonators have uniquely high Q-factors, which has led to their wide application as elements of various frequency-selective devices in infrared and optical communication systems [1–3]. Thanks to active research carried out in recent decades, the design of filters based on microresonators has reached a high level of development [4]. However, along with the indicated advantage, this type of resonators also has a well-known limitation - a quasi-periodic spectrum of frequencies of natural oscillations. To compare the spectral parameters of the resonators, the concept of the frequency distance between neighboring resonant peaks was introduced: FSR - free spectral range. The frequency distance between adjacent resonant peaks for ring microresonators is inversely proportional to their radius.

The presence of a periodic sequence of natural frequencies in microresonators with whispering gallery oscillations makes it possible to use their structure, built as a bandstop filter, to obtain the frequency characteristics of scattering as for bandpass filters. In this report, we consider the possibility of implementing bandpass filters on the structure of bandstop filter by optimizing the number of microresonators and directional changes in their FSR.

To carry out numerical studies, we have developed an electrodynamic model of a bandstop filter based on perturbation theory [5]. To reduce the coupling between adjacent microcavities, it was assumed that the filter has the form of a linear array of ring microresonators with degenerate oscillations (Fig. 1, a).

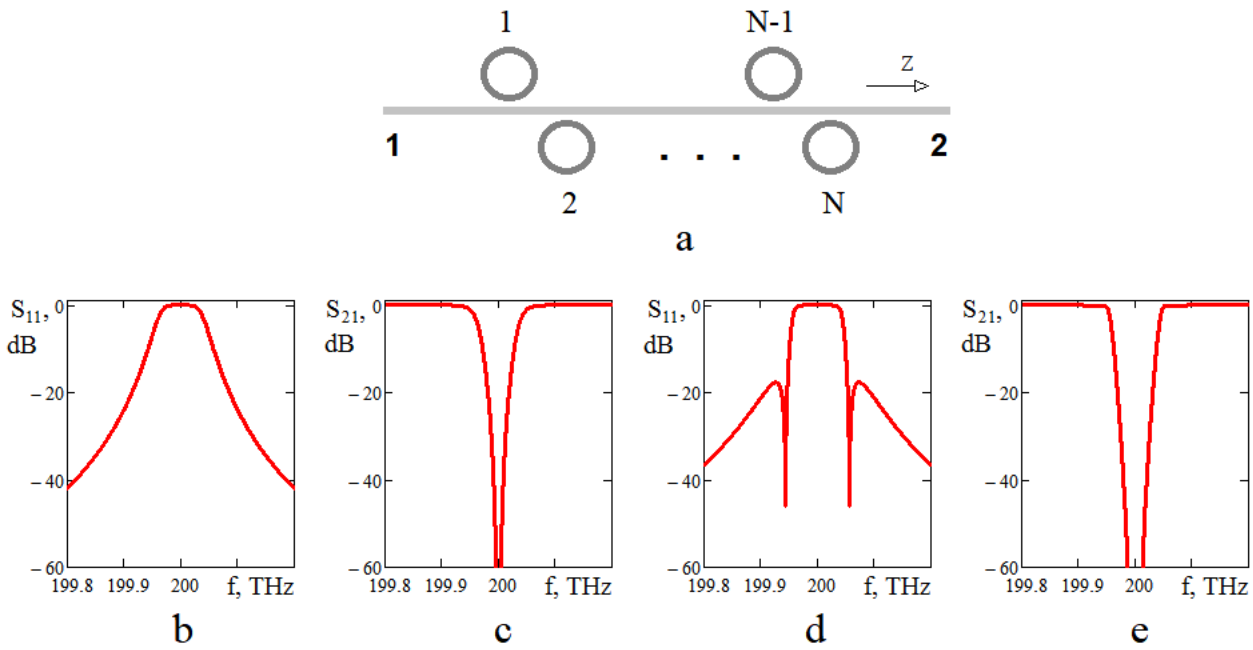


Fig. 1. Bandstop filter built on a linear array of ring microcavities (a). Scattering characteristics of bandstop filters (a) on 2 (b, c), 4 (d, e) microresonators (center frequency $f_0 = 200$ THz).

It was also assumed that neighboring microresonators are located on different sides of the transmission line at a distance $\Gamma\Delta z = (2s+1)\pi/2$ (s-integer) and are made of the same dielectric (Γ is the wave number; $\Delta z = |z_t - z_{t+1}|$; z_t is the longitudinal coordinate of the t-th resonator).

First, the scattering characteristics of structures optimized as bandstop filters were studied. (fig. 1, b - e).

At the second stage, by varying the FSR, the coupling coefficients, and the number of microresonators, we tuned and optimized the transmission parameters to the characteristic of bandpass filters (fig. 2).

As a result, we obtained the following data:

The frequency response of the first bandpass filter (fig. 2, a - d) has such parameters:

center frequency $f_0 = 199{,}880$ THz;

minimum loss in the passband -1,4 dB; -3 dB bandwidth: 560 GHz;

squareness frequency response (ratio of -30 dB bandwidth to -3 dB bandwidth) 3,7.

The frequency response of the second bandpass filter (fig. 2, e - h) is characterized by the following parameters:

center frequency 199,885 THz;

minimum loss in the passband -0,9 dB; -3 dB bandwidth: 50 GHz;

squareness of frequency response 8.

Interestingly, the narrowing of the bandwidth of the second filter did not lead to an increase in losses.

The phase-frequency dependence of both filters in the passband is close to linear (fig. 2, d, h).

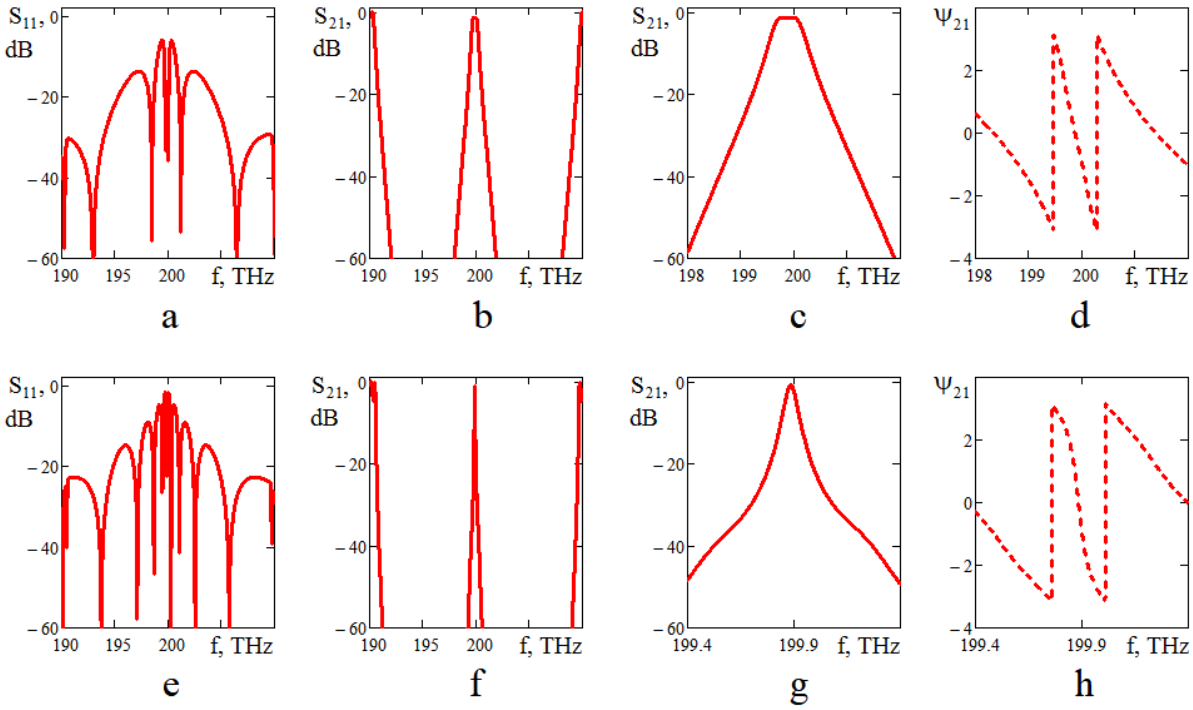


Fig. 2. Scattering characteristics of a bandpass filter based on an optimized linear array of 8 microresonators (a - d) ($N = 8$; $f_0 = 199{,}880$ THz; FSR: $\Delta f = 10$ THz;); of 14 microresonators (e - h) ($N = 14$; $f_0 = 199{,}885$ THz; FSR: $\Delta f = 9{,}6$ THz).

Thus, the obtained simulation results demonstrate the possibility of implementing a wide class bandpass filters based on barrier structures, using microresonators with whispering gallery oscillations. The proposed new type of filters can find practical application in multiplexers, amplifiers, lasers and other devices of infrared and optical communication systems.

References

1. Schwelb O. Stopband characteristics of optical Vernier filters built with microring resonators // https://www.academia.edu/en/3030237/Stopband_characteristics_of_optical_Vernier_filters_built_with_microring_resonators
2. Roeloffzen C.G.H., Zhuang L., Heideman R.G., Borreman A., Van Etten W. Ring resonator-based Tunable Optical Delay Line in LPCVD Waveguide Technology // Proceedings Symposium IEEE/LEOS Benelux Chapter, 2005, Mons. Pp. 79 – 82.
3. Poon J. K. S., Scheuer J., Yariv A. Wavelength-Selective Reflector Based on a Circular Array of Coupled Microring Resonators // IEEE Photonics Technology Letters, Vol. 16, No. 5, 2004. Pp. 1331 – 1333.
4. I. Chremmos, O. Schwelb, N. Uzunoglu. Editors. Photonic Microresonator Research and Applications. Springer International Publishing Switzerland – 2010 – 517 p.
5. A.A. Trubin. Lattices of Dielectric Resonators. Springer International Publishing Switzerland – 2016 – 171 p. https://link.springer.com/book/10.1007/978-3-319-25148-6
6. Trubin A.A. Electrodynamic modeling of Add-drop filters on optical microresonators // Information and Telecommunication Sciences, 2019, No 1, pp. 30-36. http://infotelesc.kpi.ua/article/view/172297

UDC 621.396.946

SCATTERING OF PLANE WAVES ON ONE-DIMENSIONAL LATTICES OF SPHERICAL DIELECTRIC RESONATORS

Trubin A. A.
National Technical University of Ukraine "Kyiv Polytechnic Institute"
E-mail: atrubin9@gmail.com

РОЗСІЮВАННЯ ПЛОСКИХ ЕЛЕКТРОМАГНИТНИХ ХВИЛЬ НА ОДНОВИМІРНИХ РЕШІТКАХ СФЕРИЧНИХ ДІЕЛЕКТРИЧНИХ РЕЗОНАТОРІВ

Розглядається задача розсіювання плоских електромагнітних хвиль на одновимірних решітках діелектричних резонаторів (ДР) сферичної форми з нижчими коливаннями магнітного типу H_{1m1}. На основі теорії збурень, побудована електромагнітна модель решіток. Аналізуються особливі випадки розсіювання на лінійних та кільцевих структурах. Розглянуті решітки можуть використовуватися як елементи антен в пристроях зв'язку або інтернету речей оптичного та інфрачервоного діапазонів довжин хвиль.

Today, spherical dielectric resonators (DRs) are considered as one of the main elements of various devices in the infrared and optical ranges [1-4]. Despite the fact that the fields of this type of resonators are described by relatively simple analytical expressions, the calculation of more complex structures, based on them, faces significant computational difficulties. At the same time, obtaining exact analytical solutions usually leads to cumbersome computational structures [5]. Analytical modeling using perturbation theory also makes a number of difficulties arising from the high sensitivity of the output parameters to the relative frequencies of partial resonators, as well as the uncertainty in the choice of basis functions for a spherical DRs. At the same time, the construction of electromagnetic models of such structures provides valuable information about the behavior of systems of various shapes lattices under different scattering conditions.

In this report, we considered the problem of scattering of plane waves on various one-dimensional lattices of spherical DRs with fundamental magnetic oscillations of partial resonators H_{1m1} $(m = 0, \pm 1)$. On the basis of perturbation theory [6], an electromagnetic model of scattering on one-dimensional and quasi-one-dimensional ring lattices is constructed, taking into account the excitation of degenerate oscillations of the main type in the system of resonators. Various particular cases of wave scattering are considered, which are of interest for the development of antenna field spatial converters for access points of optical and infrared communication systems.

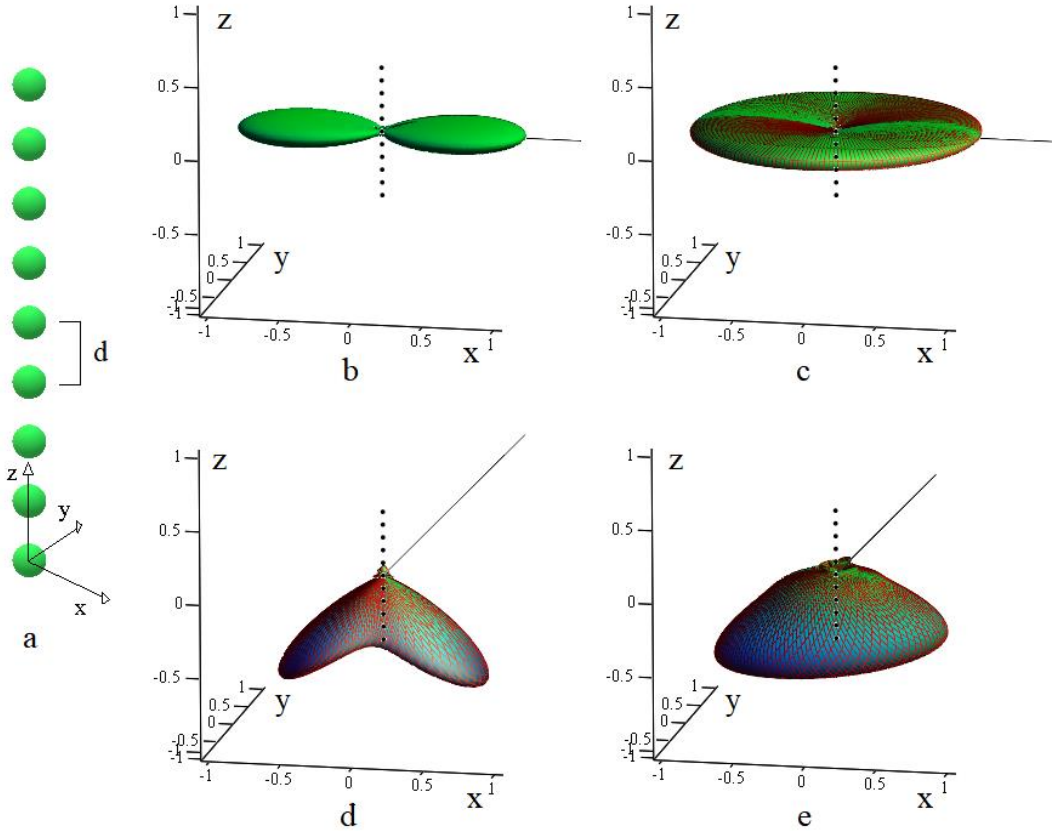


Fig. 1. Linear lattice of spherical DRs. Angular dependences of the squared modulus of scattering amplitude $\left|f\left\langle\theta_k,\varphi_k\left|\theta,\varphi\right\rangle\right.\right|^2$ for $k_0d=1/4$; $\varphi_k=\pi$; $\theta_k=\pi/2$ (b, c); $\theta_k=3\pi/4$ (d, e) for p scattering - (b, d); for s-scattering (c, e). (Straight lines show the direction of the incident wave, and the dots show the spatial arrangement of the resonators).

Expanding the scattered field of the lattice in terms of natural oscillations of the system of resonators [6], we took into account the coupling coefficients of all types of oscillations H_{1m1} $(m=0,\pm1)$ [7], differing from each other by the field rotation, near the lowest resonance frequency f_0.

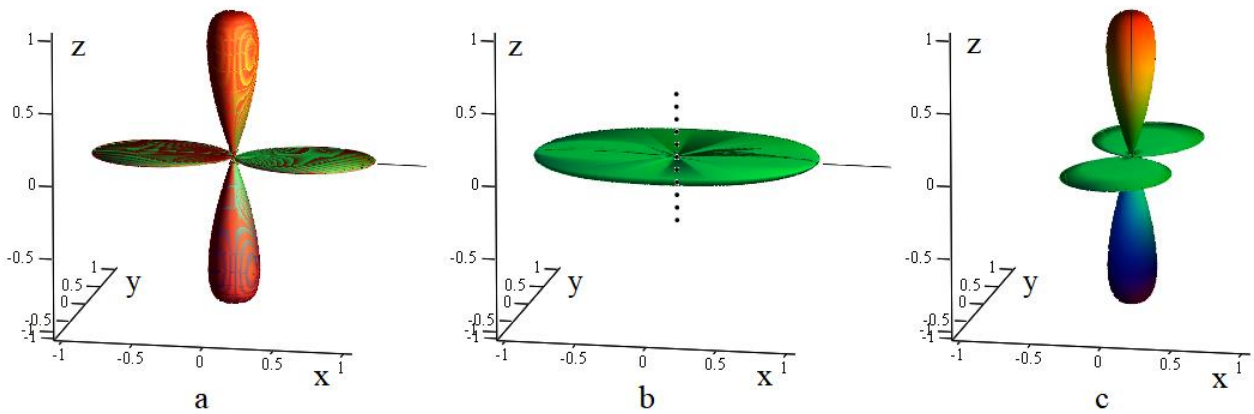


Fig. 2. Angular dependences of the squared modulus of scattering amplitude for $k_0d=1$; $\varphi_k=\pi$; $\theta_k=\pi/2$; (a, b) and for $\theta_k=\pi$ (a, c) for p scattering - (a) for s-scattering (b, c).

The noted relationship between degenerate oscillations with different values of azimuthal indices in the spatial structures of spherical DRs redistributes the lattice field in most cases, having a noticeable effect on its characteristics (see, for example, fig. 3, e). At the same time, the maximum spatial symmetry of spherical DRs makes lattices, built on their basis, as responsive as possible for different directions of incidence for waves of different polarizations, which is especially attractive for building access points in communication systems.

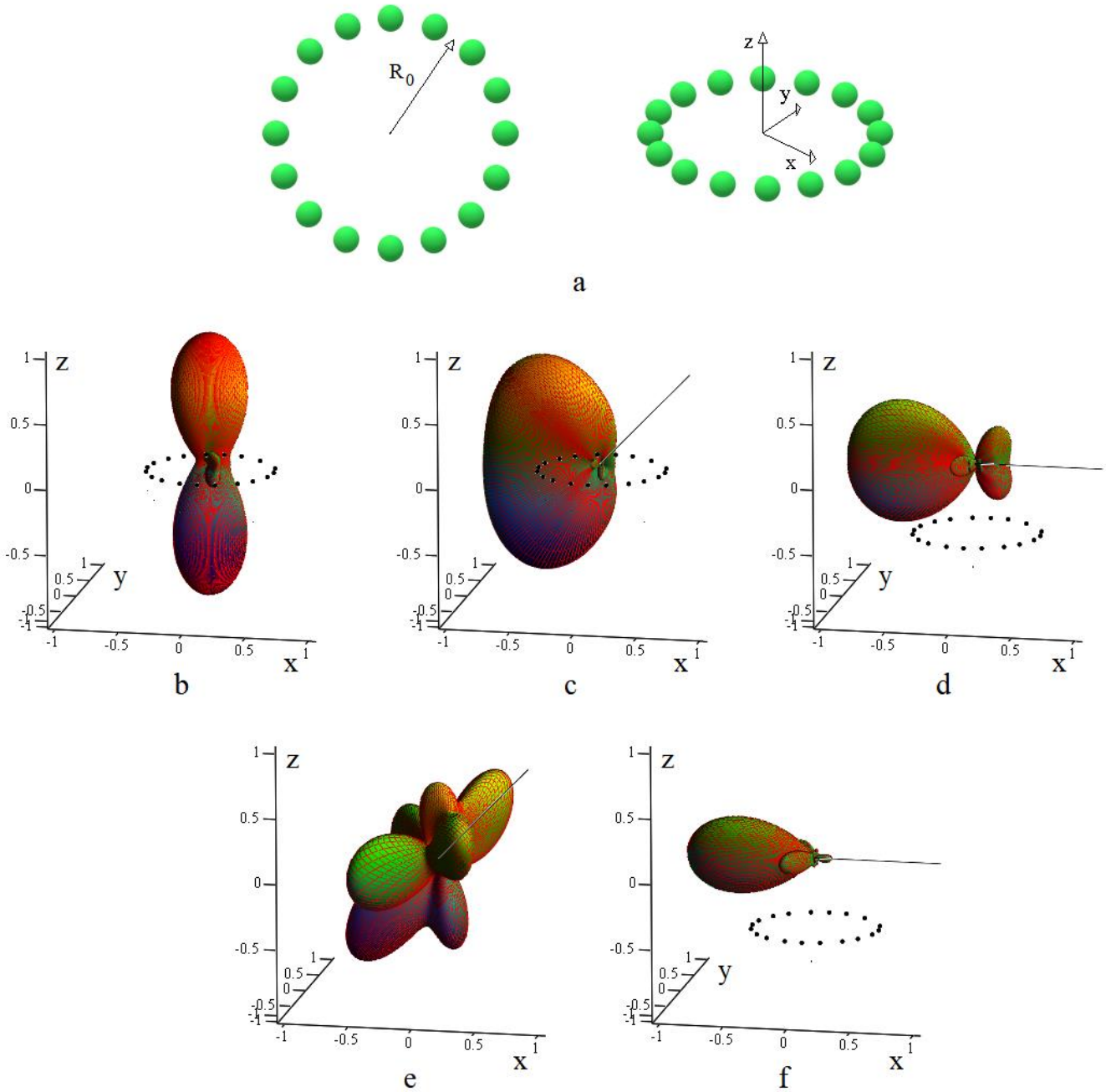


Fig. 3. Ring lattice of 16 Spherical DR (a). Angular dependences of the squared modulus of scattering amplitude for $k_0R_0 = \pi$; $\varphi_k = \pi$; $\theta_k = \pi$ (b); $\theta_k = 3\pi/4$ (c, e); $\theta_k = \pi/2$ (d, f); for p scattering - (b - d) for s-scattering (e - f).

The constructed model made it possible to calculate and analyze the scattering features of p and s type plane waves for different angles of incidence. On fig. 1-3 points show the conditional spatial arrangement of the lattices. The direction of propagation of the incident wave is shown by a solid line, defined by wave vector $\vec{k}_0$.

It was assumed that all resonators are made of a dielectric with $\varepsilon_{1r} = 36$.

As follows from the calculations, in the case of s-scattering, the incident plane wave is transformed by a linear grating into a uniformly distributed wave in azimuth (fig. 1, c; fig. 2, b) compressed in the vertical direction. In the case of p-scattering, the incident wave is scattered in directions determined by its polarization with respect to the spatial arrangement of the lattice (fig. 1, b, d; fig. 2, a; fig. 3, b - d). Interestingly, in the case of p-scattering on a linear lattice with $k_0 d = 1$, the theory predicts the same distribution of the field for two different directions of the incident wave: $\theta_k = 0$; and $\theta_k = \pi$.

Thus, the data obtained show that linear and ring lattices based on spherical DRs have a more complex field structure associated with the excitation of several types of degenerate oscillations of these type resonators. The considered structures are of practical interest for use in access and transmission systems of optical and infrared communication systems.

References

1. Molet P., Gil-Herrera L. K., Garcia-Pomar J. L., Caselli N., Blanco B., Lypez C., Mihi A. Large area metasurfaces made with spherical Silicon resonators // Nanophotonics. 2020; 9(4): pp. 943–951. https://doi.org/10.1515/nanoph-2020-0035
2. Dey U., Hesselbarth J. Spherical Dielectric Resonator Antenna Operating at 180 GHz // IEEE Antennas and Wireless Propagation Letters, Vol. 19, No. 8, August 2020. Pp. 1380 – 1384.
3. Astratov V. N. Ch. Fundamentals and Applications of Microsphere Resonator Circuits. Photonic Microresonator Research and Applications. Springer. 2010. pp. 423-457.
4. Hong S., Lee Y. J,, Moon K., Kim Y., Shin E., Kwon S-H. Far-Field Analysis on Reflecting Colors of Dielectric Nanosphere Metasurface // Hindawi Journal of Nanomaterials. Vol. 2019, Article ID 6532967, 8 pages. https://doi.org/10.1155/2019/6532967
5. Mackowsky D. W., Mishenko M. I. Calculation of the T matrix and the scattering matrix for ensembles of spheres // J. Opt. Soc. Am. / 1996. Vol. 13, No. 11. pp. 2266 - 2278.
6. A.A. Trubin Lattices of Dielectric Resonators. Springer International Publishing Switzerland – 2016 – 171 p. https://doi.org/10.1007/978-3-319-25148-6
7. Trubin A.A. Coupling coefficients of the Spherical dielectric microresonators with whispering gallery modes // Visnyk NTUU "KPI" ser. Radiotechnique, Radioaparatus Building. 2015.N.62, pp. 49-61. https://doi.org/10.20535/RADAP.2015.62.49-61

УДК 621.3

BROADBAND WIRELESS COMMUNICATION IN THE TERAHERTZ RANGE: THE KEY TO THE SUSTAINABILITY OF THE DIGITAL ECONOMY

[1]Oliinyk D.I., [2]Nizhnyi D.A.,
[1]*National Institute for Strategic Studies*
[2]*National Technical University of Ukraine*
"Igor Sikorsky Kyiv Polytechnic Institute"
E-mail: olijnukd@i.ua, nizhnyi.danyil@lll.kpi.ua

ШИРОКОСМУГОВИЙ БЕЗДРОТОВИЙ ЗВ'ЯЗОК В ТЕРАГЕРЦОВОМУ ДІАПАЗОНІ : ЗАПОРУКА СТІЙКОСТІ ЦИФРОВОЇ ЕКОНОМІКИ

У статті наводяться новітні тенденції застосування частот терагерцового діапазону для створення новітніх стійких бездротових телекомунікаційних технологій і систем наступних поколінь, які дозволяють збільшити обсяг передачі інформації, масове підключення пристроїв та безпечну передачу даних при зондуванні об'єктів з високою роздільною здатністю щодо забезпечення стійкості цифрової трансформації економіки і суспільства.

The article focuses on the latest trends in using terahertz band frequencies to create sustainable next-generation wireless telecommunications technologies and systems. These technologies and systems enable increased information transmission, mass device connectivity, and secure data transmission. Additionally, they can sense high-resolution objects for a sustainable digital transformation of the future economy.

The shared digital future of society depends on the growing number of devices, services, and products in the limited radio frequency spectrum. In Ukraine, identifying and agreeing on the availability of spectrum is crucial for achieving cost-effective deployment of communication services. Increased coverage and bandwidth are crucial within the framework of the World Radiocommunication Conference, ITU WRC-23 [1]. This conference regulates the use of radio frequency spectrum, as well as geostationary satellite and non-geostationary satellite orbits.

The terahertz (THz) electromagnetic spectrum lies between the mm-wave (*mmWave*) and far-infrared (IR) bands and provides much higher bandwidth compared to the *mmWave* band and more favorable propagation conditions compared to the IR band. THz frequencies promise to provide a wide spectrum, data transfer rates of more than a hundred gigabits per second (Gbps), mass connectivity, denser networks and highly secure data transmission. The U.S. Defense Advanced Research Projects Agency (*DARPA*) has identified THz technology as one of four major research areas. It is also considered a major component of the next phase of telecommunications. This technology may have a

greater impact on society than the Internet itself.

Among the main areas of application of the terahertz band, the International Telecommunication Union (*ITU*) has identified several main areas, namely: mobile broadband expansion (*eMBB*), machine-type communication (*mMTC*) and mobile broadband expansion (*eMBB*). *mMTC* communications and ultra-reliable low-latency communications (*uRLLC*) are defined to support a wide range of traditional and emerging applications and services anytime, anywhere [2]. With *mmWave* communication becoming an industrial standard, the *IEEE ComSoc* has emerged as a key communication platform. Given this trend, there is a growing need to explore new wireless technologies that operate in the THz range, which is the next frontier beyond *mmWave* [3].

By 2030, 6G networks are expected to be a key enabler of the intelligent information society, providing higher performance than 5G in space, air, land, and underwater networks. These networks will enable ubiquitous and unlimited wireless communication, based on the integration of various promising radio access technologies for the 6G ecosystem, including THz communication [4].

The large bandwidth available at terahertz frequencies can offload low-frequency bands and provide speeds in the multi-gigabit range for future wireless systems, enabling unprecedented levels of data transfer, including massive multicore wireless networks on a chip, terabit-per-second wireless personal networks, broadband transit for Internet access in rural areas and high-speed inter-satellite connections.

In connection with the growth of the number of telecommunication systems that use electromagnetic radiation of various frequency ranges, there is a need to create new sustainable wireless telecommunication technologies and systems. These should allow for an increase in the amount of information transmitted while maintaining an environmentally safe level of radio radiation. Already, American scientists from NASA's Jet Propulsion Laboratory (JPL) are engaged in the development and integration of aerospace warfare technologies. They have managed to achieve terahertz signal transmission at a speed of 2 Gbps over a distance of 2.03 km without a bit error rate (BER). This achievement is expected to contribute to the development of 6G and the sustainability of the digital ecosystem [5].

For the 6G ecosystem and wireless communication networks of the next generation, in the scientific literature, scientists consider the need to use subterahertz and terahertz frequency ranges from 100 GHz to 10 THz. This is necessary to provide multi-kilometer and multi-gigabit-second sub-terahertz communication for wireless transit programs [6].

The need to provide higher wireless data rates for the ever-increasing number of devices connected to a wireless network is driving the search for a spectrum of radio frequency resources that is not yet in use. The Government of Ukraine has taken the first steps to carry out the conversion of the radio frequency resource of Ukraine [7] This is aimed at improving access to the mobile Internet in the radio frequency bands of 790–960 MHz and the conditions for the compatible functioning of the radio-electronic means of special users of the radio frequency resource with the radio-electronic means of mobile communication networks.

These efforts have made it possible to conduct research on innovative communication applications in the terahertz range [8].

However, there are many technological innovations that have yet to be explored. For example, the use of machine learning algorithms in wireless networks is a promising area of research that could greatly improve network performance and efficiency. Additionally, the implementation of advanced modulation schemes, such as orthogonal frequency division multiplexing (OFDM) and filter bank multicarrier (FBMC), could provide higher spectral efficiency and better resistance to interference. Further exploration of these and other innovations could lead to significant improvements in the design and operation of future wireless systems. The prospect of large contiguous bandwidths in the communications industry is a key research area for 6G wireless communication. This is due to the need to meet the demand for ultra-high data rates in the Tbit/s range with low latency while ensuring robust co-communication and radar sensing.

THz waves are promising for use in many applications in spectroscopy and high-resolution imaging, since many forms of condensed matter, molecular compounds, vapours, and gases have different physical properties that resonate with THz waves [9]. Terahertz waves allow for non-destructive control of products and do not have an ionizing effect.

Also emerging is a concept that uses wireless frequencies for both communication and sensing capabilities, namely joint communication and sensing. Terahertz frequencies would not just transmit data, but could work like a high-precision radar system to detect objects. Thus, THz sensing can provide high-resolution maps of the environment and positioning and location information with centimeter and subcentimeter accuracy.

References

1. International cooperation. URL: https://www.ucrf.gov.ua/pres-centr/news/mizhnarodna-spivpratsia_1
2. Convergence of Broadband and Broadcast/Multicast in Maritime Information. URL: Networks https://www.sciopen.com/article_pdf/1425373508562079745.pdf
3. Sixth IEEE International Workshop on Terahertz Communications in conjunction with IEEE Global Communications Conference Thursday, 8 December 2022, 8am BRT // Rio de Janeiro, Brazil. URL: https://www.thz-comm.org/
4. 6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies. URL: https://ieeexplore.ieee.org/document/8766143
5. Researchers Achieve 2Gbps Terahertz Transmission over 2km. URL: https://www.6gworld.com/exclusives/researchers-2gbps-terahertz-transmission-2km/
6. Multi-kilometre and multi-gigabit-per-second sub-terahertz communications for wireless backhaul applications. URL: https://www.nature.com/articles/s41928-022-00897-6
7. Some issues of the conversion of the radio frequency resource of Ukraine in the public radio frequency bands: Resolution of the CMU of September 5, 2014 No. 514. URL: https://zakon.rada.gov.ua/laws/show/514-2014-%D0%BF#Text
8. On some measures to improve access to the mobile Internet: Decree of the President of Ukraine dated 07/08/2019 No. 497. URL: https://zakon.rada.gov.ua/laws/show/497/2019#Text
9. Mess- und Automatisierungstechnik. URL: https://www.vdi.de/tg-fachgesellschaften/vdi-gesellschaft-mess-und-automatisierungstechnik

УДК 621.396.96

ОСОБЛИВОСТІ І ТЕНДЕНЦІЇ ТРОПОСФЕРНИХ СИСТЕМ ЗВ'ЯЗКУ

[1]Черняк А.М., [2]Наритник Т.М., [2]Шевченко Т.А.
Національна академія Служби безпеки України
[1]Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського
E-mail: chernovandnic@gmail.com; t.narytnyk@ukr.net; its.tz91@gmail.com

FEATURES AND TRENDS OF TROPOSPHERIC COMMUNICATION SYSTEMS

It is substantiated that the most relevant for application in the Armed Forces of Ukraine and other military formations for the construction of digital telecommunication systems and special-purpose networks are stations and complexes of tropospheric communication The analysis of digital tropospheric systems of the American company Comtech Systems, which is one of the world's leading leaders in the field of tropospheric communication, and tropospheric stations, which are in service with the Armed Forces of Ukraine, has been carried out. The directions of further improvement, digitalization and development of means of tropospheric communication, in particular their noise immunity, multifunctionality, multi-option and capacity increase, are considered. It is shown that the introduction of digital signal processing and the use of digital antenna arrays and space-time processing mechanisms are the most acceptable in the context of the prospects for the use of tropospheric communication with the inexpediency of increasing the mass and size indicators of tropospheric stations and transmitter signal power.

Досвід бойових дій у ході проведення ООС (АТО) показав ряд проблемних питань з організації зв'язку в тактичній (оперативній) ланці управління. Серед основних факторів, що негативно вплинули на організацію зв'язку, слід зазначити наступні: недоцільність побудови багато інтервальних радіорелейних ліній зв'язку через складнощі при організації охорони та оборони радіорелейних станцій на територіях, що не контролюються військовими формуваннями; відсутність національної супутникової системи зв'язку та необхідність оренди трафіку у цивільних операторів зв'язку; недостатня кількість апаратних (станцій) зв'язку та відповідного особового складу в штаті військових частин для виконання поставлених завдань у складі батальйонних ротних) тактичних груп.

Це, в свою чергу, вимагає вирішити завдання щодо забезпечення високої пропускної спроможності транспортних телекомунікаційних систем спеціального призначення. В таких умовах, для забезпечення зв'язку на перший план виходять засоби, які дозволяють швидко організувати інформаційні напрямки між пунктами управління. Такими є супутникові та тропосферні станції зв'язку. Однак супутникові засоби мають недоліки: залежність від іноземного оператора, висока вартість оренди послуг, тощо. Тому, найбільш актуальними для застосування у Збройних Силах України та інших військових формуваннях для побудови цифрових телекомунікаційних систем та мереж є станції та комплекси тропосферного зв'язку [1-2].

Серед основних переваг застосування тропосферного зв'язку слід зазначити наступні: відсутність залежності від рельєфу та інших факторів місцевості; забезпечення зв'язку на велику дальність (до 200 км та більше); невеликий час на розгортання тропосферних ліній зв'язку; висока мобільність станцій на автомобільній базі, можливість встановлення обладнання на бронебазу.

До характерних особливостей тропосферних систем зв'язку відносяться:

- велике додаткове (у порівнянні з випадком поширення радіохвиль у вільному просторі) згасання радіохвиль, що для інтервалів військових тропосферних радіоліній (ТРЛ) довжиною 150-200 км може складати 60-80 дБ. Додаткове ослаблення істотно

збільшується з ростом довжини інтервалу (1-1,5 дБ на 10 км зв'язку);

- істотна нестаціонарність поля в точці прийому, що зв'язано з багатопроменевістю сигналу у сполученні з рухливістю неоднорідностей та зі зміною метеоумов в об'ємі перевипромінювання .

Компанія Comtech Systems взяла активну участь в модернізації тропосферних станцій. Перше оновлення передбачало збільшення пропускної здатності даних з 2 Мбіт/с до 8 Мбіт/с в AN/TRC-170 з використанням цифрового тропосферного модему CS6716, який підтримував корекцію помилок і управління адаптацією по потужності. Друге оновлення для тропосферних станцій AN/TRC-170 передбачало збільшення пропускної спроможності до 16 Мбіт/с і створення більш мобільних антенних постів, які дозволяли б розгортання заобрійного зв'язку протягом 30–45 хвилин двома членами екіпажу, замість 6 годин 6–8 членами екіпажу, що було раніше нормою для AN/TRC-170S.

Станом на сьогодення на озброєнні ЗС України знаходяться, в основному, модернізовані мобільні цифрові тропосферні станції з встановленням на військовому вантажному засобі двох антено-поворотних обладнань (рис. 1).

Рис. 1. Тропосферна станція Р-412Б - мобільний варіант на броне базі

Модульна конструкція станцій покращує умови ремонтопридатності та дозволяє за 1-3 хвилини з допомогою автоматичної сигналізації визначити несправність та замінити модуль, що вийшов з ладу. В деяких системах забезпечується автоматичне перемикання несправного модуля на резервний.

В країнах НАТО для вирішення проблеми завадозахищеності радіорелейних та тропосферних засобів використовуються гостронаправлені антени, зменшуються рівні бокового та заднього випромінювань, створюються антени з керованим нулем діаграми направленості, шукаються можливості керування променем випромінювання антени, а також використовуються складні сигнали, методи завадостійкого кодування, завадозахищені модеми, адаптація по потужності передавачів, впроваджується апаратура контролю та визначення завад з візуальним їх відображенням, вишукуються інженерно-технічні шляхи для створення завадозахищених багатопроменевих антенних систем.

Подальше вдосконалення засобів тропосферного зв’язку, за поглядами закордонних і вітчизняних спеціалістів, направлено на прискорене впровадження цифрових методів передавання сигналів, продовження створення уніфікованих типів апаратури, що складаються з декількох модифікацій, використання єдиних засобів тропосферного зв’язку для військових, урядових та комерційних цілей, подальше підвищення розвід- і завадо захищеної роботи, збільшення пропускної спроможності, удосконалення роботи в режимі прямої видимості при пониженій потужності випромінювання, використання крім рознесеного прийому комбінованих способів боротьби з багатопроменевістю, в тому числі адаптивні модеми, метод прямої корекції помилок, що дозволить підвищити ефективність використання частотного спектру.

Кількість функцій та опцій того чи іншого пристрою більшою мірою визначається програмуванням меншою мірою апаратно і спрямоване на зручність користування послугами, тому стало можливим нівелювання вартості одно-і багатофункціональних пристроїв, що і послужило каталізатором розвитку цього напрямку. Дуже ефектним і перспективним є розвиток такого напряму в тропосферному зв’язку тропосферного зв’язку як пакетний метод передачі інформації. З техніко-економічної точки зору впровадження даного методу обумовлено простотою і зручністю користування

інтерфейсом засобів тропосферного зв'язку для стикування з кінцевим обладнанням користувача, що, безсумнівно, благотворно позначається на економічних показниках. На сьогоднішній день найбільшого поширення набула пакетна технологія IP/Ethernet, в якій незалежно один від одного поєднуються обробка TDM-трафіку (по суті, крос-комутація TDM-потоків) та механізм Ethernet-комутації для передачі Ethernet-кадрів. Дану систему вигідно відрізняє більш висока ефективність передачі інформації (надання TDM-послуги з продуктивністю як і в TDM-радіо), мінімальний час затримки, що вноситься системою, поліпшення параметрів FER (Frame Error Ratio – частота появи помилок кадру) [6-7].

Висновки. Найбільш прийнятною в контексті перспектив застосування тропосферного зв'язку при недоцільності збільшення масогабаритних показників тропосферних станції та енергії сигналу передавача, на перший план у проблемі підвищення пропускної спроможності тропосферних ліній зв'язку є впровадження цифрової обробки сигналів та використання цифрових антенних решіток і механізмів просторово-часової обробки (Space-Time Processing – STP) сигналів.

З метою набуття спроможності щодо забезпечення тропосферного зв'язку в інтересах ЗС України військовими частинами (підрозділами) зв'язку доцільно розробити (переопрацювати) нормативно- правові документи щодо розвитку та функціонування тропосферного зв'язку в Україні і провести переоснащення підрозділів ЗС України сучасними засобами тропосферного зв'язку вітчизняного та (або) закордонного виробництва. Виконання запропонованих заходів дозволить використовувати тропосферний зв'язок для побудови резервних тропосферних ліній зв'язку, або прямих напрямків в інтересах рухомих пунктів управління Збройних Сил України.

Підбиваючи підсумки вище викладеного, можна сказати, що в найближчому майбутньому тропосферний зв'язок не втратить свого значення і далі займатиме гідне місце в телекомунікаційній системі для забезпечення держави новітніми вітчизняними зразками озброєння на виконання розпорядження Кабінету Міністрів України від 30.08.2017р. №600 «Деякі питання розвитку критичних технологій у сфері виробництва озброєння та військової техніки» за напрямом «*Технології тропосферного зв'язку»*.

Література

1 . Наритник Т.М., Волков В.В., УткІн Ю.В. РадІорелейні і тропосферні системи передачі. Навч. посібник. // Видавництво „Основа", К: 2008.- 696 с.

2. Тропосферний зв'язок. Тропосферний радіорелейна лінія зв'язку «Північ» [Електронний ресурс] – Режим доступу до ресурсу: https://hi-news.pp.ua/tehnka-tehnologyi/4601-troposferniy-zvyazok-troposferniy-radoreleyna-lnya-zvyazku-pvnch.html.

3. Спосіб тропосферного зв'язку Патент України на корисну модель №108632, дата публікації 15.07.2016р., Бюл.№14 з пріоритетом від 29.01.2016 Ільченко М.Ю., Наритник Т.М., Слюсар В.І.

4. Наритник Т. М., Почерняєв В. М., Повхліб В. С.Цифрові радіорелейні та тропосферні лінії зв'язку (основи розрахунку). – Одеса: ОНАЗ ім. О.С. Попова, 2019. – 166с.

5. Масесов М. О. Перспективи застосування цифрового діаграмоутворення у станціях тропосферного зв'язку спеціального призначення / М. О. Масесов, І. Ю. Субач, Д. М. Руденко, О. В. Станович. // Збірник наукових праць ВІТІ ДУТ.– 2014. – No1. – С. 43–48.

6. Наритник Т.М. Аналітичний огляд сучасних технологій тропосферного та радіорелейного зв'язку Наритник Т.М., Ветошко І.П., Семерій С.І., Сайко В.Г., Сарапулов С.В./ Вісник університету «Україна» № 2 (23), 2019.Серія Інформатика, обчислювальна техніка, кібернетика.-С. 105-120.

7. Слюсар В.І., Масесов М.О. Ідеологія побудови перспективних тропосферних (радіорелейних) станцій спеціального призначення.// Збірник наукових праць ВІТІ НТУУ "КПІ". – 2010. – Вип. 2. - С. 114 -120. - http://www.slyusar.kiev.ua/VITI_02_2010.pdf.

УДК 629.783

РОЗРОБЛЕННЯ МАКЕТУ ДЛЯ ДОСЛІДЖЕННЯ ПРИЙМАЧІВ СИСТЕМ СУПУТНИКОВОЇ РАДІОНАВІГАЦІЇ

Ніконенко В.О., Авдєєнко Г.Л.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: nikonenko.v01@gmail.com

DEVELOPMENT OF A MODEL FOR RESEARCH RECEIVERS OF SATELLITE NAVIGATION SYSTEMS

A version of the layout project for the study of radio receivers of satellite navigation systems is presented, which is supposed to be developed on the basis of SDR technologies for the educational process of the Institute of Telecommunication Systems. The thesis is of interest to specialists in the field of satellite radio navigation.

Супутникові радіонавігаційні системи (СРНС) GPS, ГЛОНАСС та Galileo стали частиною нашого повсякденного життя. Вони дозволяють нам орієнтуватися на незнайомій місцевості, відстежувати транспорті засоби, транслювати місце знаходження інших людей та виконують інші дії. Приймачі навігаційних сигналів виконують вирішальну роль у цих системах, оскільки саме вони захоплюють та обробляють (декодують) сигнали від навігаційних супутників (НС), які містять ефемеріди – інформацію про місце знаходження НС та час передачі сигналу. Приймач використовує цю інформацію для обчислення положення користувача на поверхні Землі. У загальному випадку для визначення координат ($x_c(t)$, $y_c(t)$, $z_c(t)$) місця розташування об’єкта в просторі приймачеві необхідно провести вимірювання псевдодальностей $\Delta D_1(t)\ldots\ \Delta D_4(t)$ до чотирьох НС. При цьому отримаємо класичну систему з чотирьох рівнянь, рішення якої дозволить обчислити чотири невідомих ($x_c(t)$, $y_c(t)$, $z_c(t)$, Δt) [1]:

$$\Delta D_i(t) = D_i(t) + c\Delta t = \sqrt{\left(x_{HC.i}(t) - x_c(t)\right)^2 + \left(y_{HC.i}(t) - y_c(t)\right)^2 + \left(z_{HC.i}(t) - z_c(t)\right)^2}\ , i = \overline{1,4} \qquad (1)$$

де $x_{HC.i}(t)$, $y_{HC.i}(t)$, $z_{HC.i}(t)$ – поточні координати НС, що передаються навігаційному приймачу споживача в інформаційному службовому повідомленні від НС; Δt – часова розбіжність (розсинхронізація) шкал між НС та навігаційним приймачем; $D_i(t)$ – дійсне значення дальності до i-го НС від приймача, $i = \overline{1,4}$; c – швидкість поширення електромагнітних хвиль.

До найбільш серйозних проблем, з якими стикаються приймачі сигналів СРНС, є погіршення сигналу через різні фактори навколишнього середовища: атмосферні умови поширення радіохвиль, кількість НС, «видимих» антеною приймача, будь-які штучні перешкоди між НС та приймачем, такі як будівлі чи дерева.

Проводячи сучасні дослідження, науковці розробили низку методів для покращення продуктивності приймачів сигналів СРНС. Наприклад, метод адаптивної фільтрації можна використовувати для зменшення впливу багатопроменевих сигналів, які виникають під час відбиття сигналу від

різних поверхонь, до того як його захоплює приймач сигналу [2].

Також, для покращення продуктивності приймачів сигналів СРНС широко використовують метод цифрової обробки. Даний метод може бути використаний для покращення якості сигналу, зменшення шуму та підвищення потужності сигналу [3].

Кількість видимих супутників і геометрія їх розташування відносно приймача сигналу також мають значний вплив на точність визначення місцеположення об'єктів по сигналах СРНС. Для забезпечення більш надійної роботи приймачів в роботі [4] була запропонована методологія вибору «оптимальних» НС для GPS-позиціонування.

Іншими важливими аспектами приймачів сигналів СРНС є їх здатність працювати в різних середовищах і за різних умов. Найактуальнішими сучасними розробками є приймачі для сфер, які розвиваються, таких як авіація, морське, військове та космічне використання. Однією з таких робіт є розробка висотного приймача GPS для навігації космічного корабля [5]. Такий приймач може надійно працювати в складних умовах космосу.

Крім того, дослідження та розробки в приймачах сигналів СРНС, зосереджені на розширенні їх можливостей та підтримки нових програм, наприклад автономне водіння [6]. Такі технології можуть бути реалізовані в тому випадку, якщо буде забезпечена точна та надійна інформація про місце знаходження.

Отже, вищевказані приклади показують, що розвиток СРНС в частині розробки СРНС-приймачів та удосконалення обробки сигналів у них є актуальною та своєчасною задачею. У зв'язку з цим вважаємо, що необхідно посилити практичну компоненту у вивченні принципів формування навігаційних сигналів та їх оброблення в навігаційних приймачах. На даний момент часу авторами відповідно до структурної схеми, що зображена на рис.1, вже розроблено для навчального процесу декілька макетів СРНС-приймачів на базі навігаційних модулів від компаній SIMCom, LOCOSYS та інш., які підтвердили свою працездатність [7].

Недоліком розроблених макетів [7] є необхідність їх встановлення або поза навчальної лабораторії, або на підвіконні лабораторії, тобто там, де є надійний прийом навігаційних сигналів. З іншого боку в розроблених макетах немає можливості керувати параметрами прийнятих навігаційних сигналів, що не дозволяє дослідити вплив цих параметрів на режими роботи навігаційних приймачів. У зв'язку з цим автори пропонують доповнити вже наявні макети [7] на рис.1 джерелом формування навігаційних сигналів на базі
SDR-трансивера (наприкад, BladeRFx40), що буде підключений до персонального комп'ютеру (ноутбука) і працюватиме під керівництвом операційної системи Ubuntu. Такий підхід, по-перше, дозволить розміщувати СНРС-приймач у будь-якому місці навчальної лабораторії, забезпечуючи зручність проведення занять, а по-друге забезпечуватиме гнучке керування кількістю навігаційних сигналів та їх параметрами, імітуючи різні варіанти поширення сигналів з подальшим дослідженням роботи СРНС-приймачів.

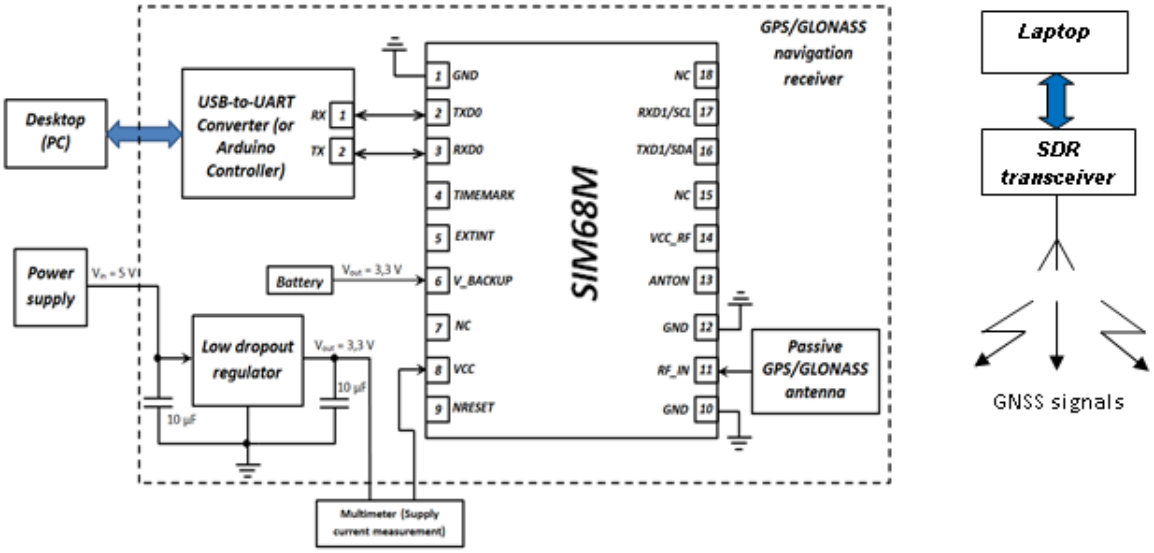


Рис. 1. Стуктурна схема СРНС приймача на базі навігаційного модуля SIMCom SIM68M.

Формування сигналів СРНС GPS та/або GLONASS відбуватиметься у програмному середовищі GNURadio для діапазону L1, які випромінюватимуться в межах навчальної лабораторії і прийматимуться наявними макетами СРНС-приймачів з подальшою обробкою та візуалізацією координат місцеположення об’єкта та інших параметрів за допомогою спеціалізованого програмного забезпечення.

Література

1. Супутникові радіонавігаційні системи : навчальний посібник / авт.кол. : І. В. Корнієнко, В.І. Богом’я, О.І. Терещук, С П. Корнієнко. Чернігів: Черніг. нац. технол. ун-т, 2014. 280 с.
2. L. Cheng, K. Wang, M. Ren and G. Yan, "Adaptive Filter Approach for GPS Multipath Estimation Under Correntropy Criterion in Dynamic Multipath Environment," in IEEE Transactions on Signal Processing, vol. 67, no. 22, pp. 5798-5810, 15 Nov.15, 2019, doi: 10.1109/TSP.2019.2946028.
3. C. Fernández-Prades, J. Arribas and P. Closas, "Robust GNSS Receivers by Array Signal Processing: Theory and Implementation," in Proceedings of the IEEE, vol. 104, no. 6, pp. 1207-1220, June 2016, doi: 10.1109/JPROC.2016.2532963.
4. F.M. Jumaah, A.A. Zadain, B.B. Zaidan, A.K. Hamzah, R. Bahbibi, “Decision-making solution based multi-measurement design parameter for optimization of GPS receiver tracking channels in static and dynamic real-time positioning multipath environment”, Measurement, Volume 118, 2018, Pages 83-95, ISSN 0263-2241
5. Winternitz, Luke B., Bamford, William A., Price, Samuel R., "New High-Altitude GPS Navigation Results from the Magnetospheric Multiscale Spacecraft and Simulations at Lunar Distances," Proceedings of the 30th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2017), Portland, Oregon, September 2017, pp. 1114-1126.
6. Xing Liu, Tarig Ballal and Tareq Y. Al-Naffouri Computer, Electrical and Mathematical Science and Engineering Division King Abdullah University of Science and Technology (KAUST) Thuwal, Saudi Arabia, 2019.
7. Гончаренко О. М., Авдєєнко Г. Л. Приймач сигналів супутникової навігації GPS//XII Міжнародна науково-технічна конференція «Проблеми телекомунікацій» ПТ-2018: Збірник матеріалів конференції. К.: КПІ ім. Ігоря Сікорського, 2018. – 498 с., с.417-420.

УДК 621.391

АНАЛІЗ ЗАВАДОСТІЙКОСТІ АЛГОРИТМУ ВХОДЖЕННЯ В СИНХРОНІЗМ РАДІОЛІНІЇ З ППРЧ НА ОСНОВІ ОЦІНКИ ФАЗИ *M*-ПОСЛІДОВНОСТІ

Василенко С. В., Єрохін В. Ф., Зінченко Я. В.
Інститут спеціального зв'язку та захисту інформації
Національного технічного університету України
"Київський політехнічний інститут імені Ігоря Сікорського", Україна
E-mail: vasylenko.phd@gmail.com

ANALYSIS OF INTERFERENCE RESISTANCE OF THE ALGORITHM OF ENTERING INTO SYNCHRONISM RADIO LINE WITH FHSS ON THE BASIS OF *M*-SEQUENCE PHASE DETERMINATION

In this paper analysis of interference resistance of the algorithm of entering into synchronism radio line with frequency-hopping spectrum spreading (FHSS) on the basis of *M*-sequence phase determination, which allows to optimize the time of entering synchronization with the given requirements of the probability of entering synchronization, or to solve the inverse problem of selection number of frequencies required for entering synchronization and generator register length of the pseudo-random sequence (PRS).

Системи радіозв'язку (СРЗ) постійно змушені функціонувати у складній радіоелектронній обстановці, яка зумовлюється як природними так і навмисними завадами, що діють в каналі зв'язку. Одним з ефективних методів захисту СРЗ від навмисних завад є використання широкосмугових сигналів з псевдовипадковим переналаштуванням робочої частоти (ППРЧ).

Оскільки прийом та обробка широкосмугових сигналів з ППРЧ вимагає точної синхронізації між опорною та прийнятою псевдовипадковими послідовностями (ПВП), на приймальній стороні повинні вживатися заходи для співпадання у часі опорної та прийнятої ПВП, а також підтримці цього стану [1-2].

У роботі проведено аналіз алгоритму входження в синхронізм радіолінії з ППРЧ, що ґрунтується на способі визначення фази *M*-послідовність на будь-якому $(i+l)$-ому такті роботи на основі прийнятих наборів відрізків *M*-послідовності, сума символів яких не менше довжини регістра генератора ПВП [3].

З метою забезпечення можливості аналізу завадостійкості, процес входження в синхронізм радіолінії з ППРЧ був представлений у вигляді графу станів, де вузли графа характеризують стан системи синхронізації радіолінії з ППРЧ, а переходи – події. У роботі, як приклад, наведено граф станів процесу входження в синхронізм радіолінії з ППЧР для довжини регістру $n=9$ та кількості частот входження в синхронізм $k=8$ (рис. 1).

На графі p_0 – ймовірність тактової синхронізації, а $p_{\Sigma 1}=\frac{1}{k}p_0\sum_{i=1}^{n}\left(1-\frac{1}{k}p_0\right)^{i-1}$, $p_{\Sigma 2}=\frac{1}{k}p_0\sum_{i=2}^{n}\left(1-\frac{1}{k}p_0\right)^{i-1}$, $p_{\Sigma 3}=\frac{1}{k}p_0\sum_{i=3}^{n}\left(1-\frac{1}{k}p_0\right)^{i-1}$.

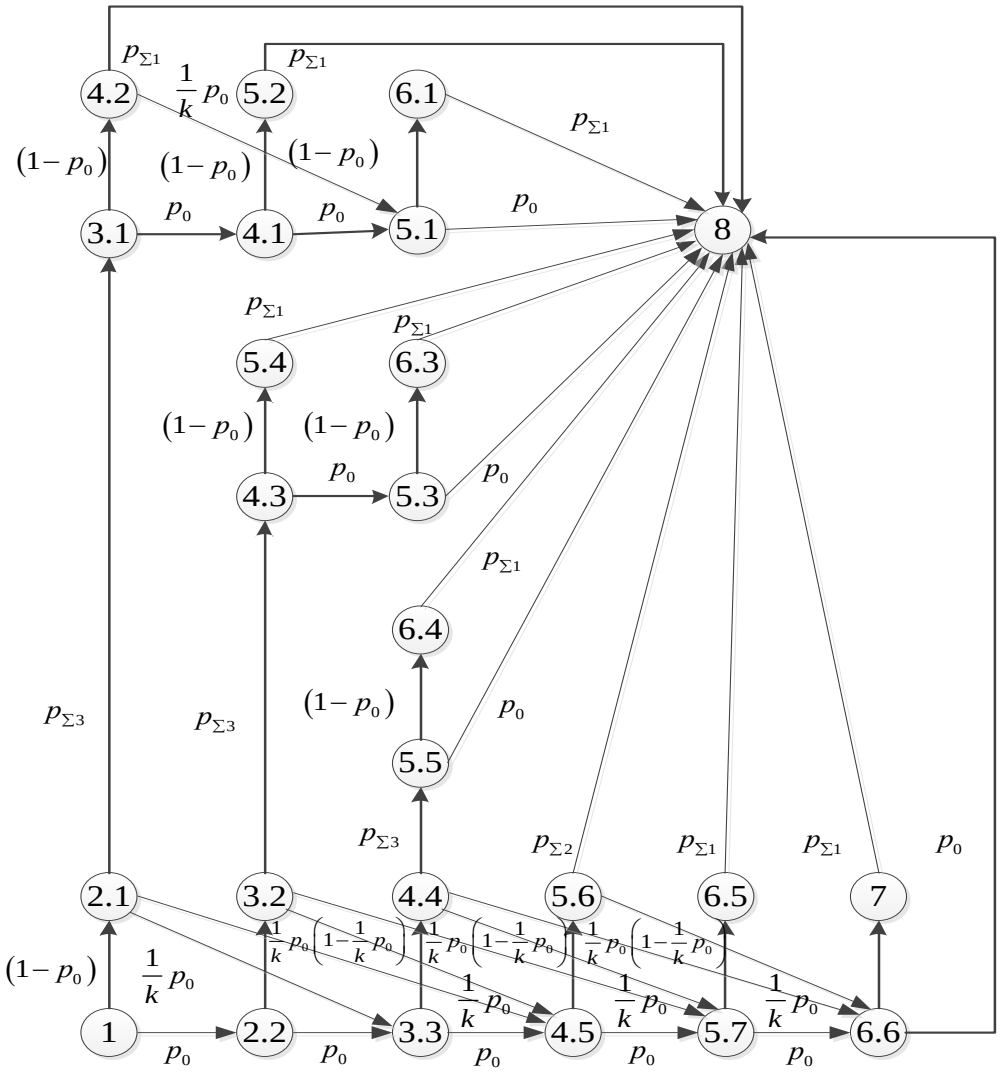


Рис. 1. Граф станів процесу входження в синхронізм радіолінії з ППРЧ

Стану 1 графа відповідає стан початкового приймання сигналу передавача (перше співпадання частот передачі та прийому, а також правильної тактової синхронізації).

Станам 2.2, 3.3, 4.5, 5.7, 6.6 відповідають стани прийому сигналу, при якому пам'ять процесора заповнюється послідовно (без пропусків у часі).

Стани 2.1, 3.2, 4.2, 4.4, 5.2, 5.6, 6.5, 7, 5.2, 6.1, 5.4, 6.3, 6.4 характеризують неприйняття сигналу та переналаштування приймача на кращу частоту.

Стани 3.1, 4.3, 5,5 характеризують прийом сигналу передавача, у якому пам'ять процесора заповнюється не послідовно, а з деякими пропусками. Тобто між відомими (прийнятими) сегментами виявляються більше одного невідомих (неприйнятих) субелементів.

Стан 8 характеризує повне заповнення регістру генератора ПВП або прийом набору сегментів *M*-послідовності, сума субелементів яких не менше довжини регістра генератора ПВП.

Разом з цим при розрахунку ймовірності входження в синхронізм (P_c) до радіолінії з ППРЧ були висунуті такі обмеження: довжина регістру

генератора ПВП $n=[8;\ 9]$; кількість частот входження в синхронізм $k=8$; кількість тактів входження в синхронізм $N=[5,\ 50]$; ймовірності тактової синхронізації $p_0=[0.01,\ 0.999]$.

Результати розрахунків були представлені у вигляді графіків залежності $P_c = f(p_0)$ при фіксованих значеннях N (рис. 2) та $P_c = f(N)$ для фіксованих значень p_0, та $n=9$ і $n=8$ (рис. 3).

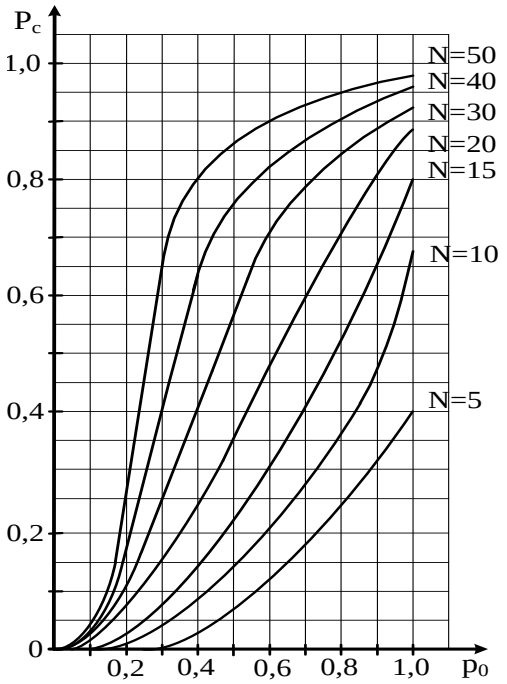


Рис. 2. Графіки залежності $P_c = f(p_0)$

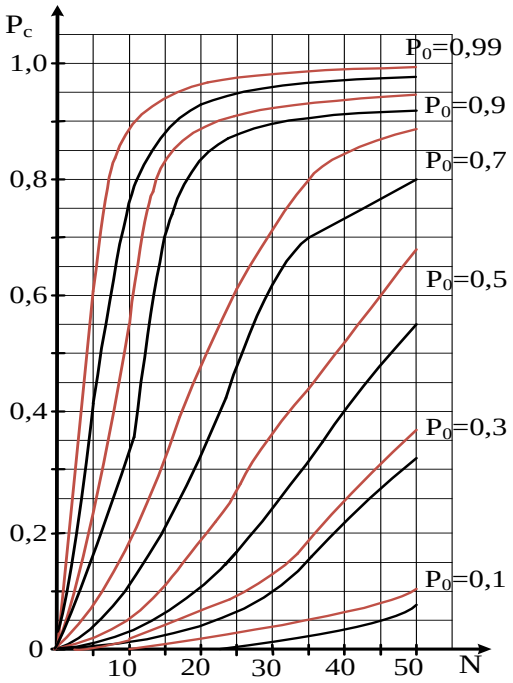


Рис. 3. Графіки залежності $P_c = f(N)$

Аналіз результатів представлених на рис. 2-3 дозволяє стверджувати, що:

досягнення значень $P_c \approx 1$, навіть при великих значеннях p_0, без збільшення кількості частот входження в синхронізм k не можливе;

використання $N > 30$ при $p_0 = [0{,}9;\ 0{,}99]$ недоцільно, оскільки призводить до збільшення часу входження в синхронізм при незначному збільшенні P_c;

зменшення довжини регістру генератора ПВП з $n=9$ (верхні криві рис. 3) до $n=8$ (нижні криві рис. 3) для значень $p_0 = [0{,}9;\ 0{,}99]$ не призводить до значного збільшення значення P_c.

Література

1. Лосев В. В., Бродская Е. Б., Коржик В. И. Поиск и декодирование сложных дискретных сигналов. Москва : *Радио и связь*, 1988. С 224.
2. Свириденко С. С. Основы синхронизации при приеме дискретных сигналов. Москва : *Связь*, 1974. С 144.
3. Василенко С. В. Алгоритм входження в синхронізм радіолінії з ППРЧ на основі визначення фази М-послідовності. *Перспективи телекомунікацій* : матеріали XVI Міжнар. наук.-техн. конф., 11–15 квіт. 2022 р. Київ : КПІ ім. Ігоря Сікорського, 2022. С. 106–108.

УДК 621.382

ОГЛЯД СУЧАСНИХ ТЕХНОЛОГІЙ ЦИФРОВОГО ТЕЛЕВІЗІЙНОГО МОВЛЕННЯ

Кисіль А. В., Авдєєнко Г. Л.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: linka.kisel2002@gmail.com

OVERVIEW OF MODERN TECHNOLOGIES OF DIGITAL TELEVISION BROADCAST

A brief overview of modern standards and technologies of digital television broadcasting is presented: DVB, HbbTV, ATSC, IPTV, OTT.

Сьогодні цифрове телевізійне мовлення є однією з основних технологій у сфері телекомунікацій та масової комунікації. Цифрове телебачення забезпечує кращу якість зображення та звуку, більшу кількість каналів і можливість передачі контенту високої чіткості (HD) і надвисокої чіткості (4K). Нижче наведено огляд деяких сучасних технологій цифрового телевізійного мовлення.

1. DVB (цифрове відеомовлення).

DVB – міжнародний стандарт, який використовується для цифрового телевізійного мовлення. Стандарт DVB охоплює різні технології цифрового телебачення, включаючи DVB-S/S2 (супутникове мовлення), DVB-T/T2 (наземне мовлення) і DVB-C (кабельне мовлення).

- Цифрове телебачення DVB-T2 – це стандарт цифрового наземного телевізійного мовлення другого покоління. Однією з ключових переваг DVB-T2 є його здатність передавати більше каналів у заданій смузі радіочастотного каналу порівняно з DVB-T, що призводить до більш ефективного використання спектру. Це дозволяє надати глядачам більший вибір каналів і програм.

- Кабельне телебачення DVB-C – європейський стандарт цифрового телебачення трансльованого за допомогою кабелю. Кабельне телебачення дає надійний за якістю сигнал, адже жоден спосіб бездротової передачі даних не може бути ефективніше, ніж кабель. По кабелю картинка завжди буде чіткою і без перешкод [1].

- Супутникове телебачення DVB-S - це стандарт, який використовується для супутникового телевізійного мовлення, що дозволяє передавати цифрові відео та аудіосигнали через супутник. Для прийому передач DVB-S вам потрібна супутникова антена, спрямована на супутник, що транслює сигнал, супутниковий приймач, який може декодувати цифрові сигнали, і телевізор або інший пристрій відображення для перегляду програм [2].

2. HbbTV (гібридне широкосмугове мовлення)

HbbTV – це стандарт, який поєднує традиційне телебачення та Інтернет. HbbTV дозволяє користувачам дивитися телепрограми та взаємодіяти з

Інтернетом за допомогою одного пристрою. Користувачі можуть переглядати відео за запитом, переглядати веб-сторінки та користуватися різними сервісами.

3. ATSC 3.0 (Комітет з передових телевізійних систем 3.0)

ATSC 3.0 — це нова версія стандарту ATSC, яка була представлена в Сполучених Штатах у 2020 році. ATSC 3.0 забезпечує вищу якість відео та аудіо, покращує прийом та інтерактивність, включаючи цільову рекламу та персоналізований контент. ATSC 3.0 також сумісний з мобільними пристроями та дозволяє більш ефективно використовувати спектр, що може призвести до створення нових послуг і додатків.

4. IPTV (Internet Protocol Television)

IPTV – це технологія, яка дозволяє транслювати телевізійний контент через Інтернет-протокол (IP). IPTV надає користувачеві можливість переглядати телепрограму в будь-який час та в будь-якому місці, що робить її дуже зручною та доступною.

Щоб використовувати IPTV, глядачам зазвичай потрібна телевізійна приставка або смарт-телевізор із вбудованими можливостями IPTV, а також підключення до Інтернету з достатньою пропускною здатністю для обробки потокового відеовмісту [3].

Однією з головних переваг IPTV є його гнучкість і універсальність. Це дозволяє глядачам отримувати доступ до телевізійних програм практично з будь-якого місця, де є підключення до Інтернету, що робить його особливо корисним для мандрівників або людей, які живуть у районах з обмеженим доступом до традиційних телевізійних послуг. Крім того, оскільки IPTV використовує Інтернет-протоколи, його можна легко інтегрувати з іншими інтернет-сервісами, такими як веб-перегляд, електронна пошта та соціальні мережі.

5. OTT (Over-The-Top) – це технологія, що використовується в цифровому телевізійному мовленні, яка дозволяє користувачам отримувати доступ до телевізійного вмісту через Інтернет без необхідності підписки на традиційне кабельне або супутникове телебачення. Послуги OTT надаються через широкосмугові мережі, і користувачі можуть отримати до них доступ через різні пристрої, такі як смартфони, планшети, смарт-телевізори та потокові пристрої.

Однією з переваг технології OTT є те, що вона надає користувачам більше контролю над тим, що вони дивляться та коли вони це дивляться. Користувачі можуть отримати доступ до різноманітного контенту на вимогу та послуг потокового передавання, які можуть бути недоступні через традиційну підписку на телебачення. Послуги OTV також дозволяють надавати більш персоналізовані рекомендації щодо вмісту та можуть надати користувачам більш інтерактивний досвід перегляду [4].

Однак однією з проблем технології OTT є необхідність надійного та високошвидкісного підключення до Інтернету. Без хорошого підключення до Інтернету користувачі можуть зіткнутися з буферизацією, повільним часом завантаження та низькою якістю відео. Крім того, оскільки послуги OTT

покладаються на широкосмугові мережі, вони можуть бути більш сприйнятливими до збоїв або збоїв під час високого трафіку мережі або технічного обслуговування.

Отже, послуги OTT та IPTV забезпечують більшу гнучкість і зручність, оскільки дозволяють дивитися ТБ на вимогу та на різних пристроях.

Варіант цифрового ефірного телебачення DVB-T2 відмінно підійде для тих, хто дивиться певні канали типу центральних, на яких є як новинний контент, так і розважальний (за це не стягується абонплата) .

Супутниковий ТБ - комплект підійде жителям селищ котеджного типу або в сільській місцевості, адже доступний в тих географічних районах, де немає телецентрів або кабельного телебачення та надає найширший спектр каналів та послуг.

Кабельне та супутникове телебачення може бути більш надійним і надавати більший діапазон каналів, але все ж максимально "набирає обертів" у своєму розвитку Інтернет-телебачення.

Отже, враховуючи вищезазначене, можна сказати про актуальність практичного вивчення особливостей технічної реалізації сучасних мереж телевізійного мовлення різних технологій для підвищення рівня підготовки студентів за спеціальністю 172 «Телекомунікації та радіотехніка», яких готує навчально-науковий інститут телекомунікаційних систем. З цією метою авторкою тезису разом з керівником її дипломної роботи пропонується варіант лабораторного макету для дослідження прийому сигналів цифрового телевізійного мовлення стандартів DVB-S/S2, DVB-T/T2, DVB-C на основі застосування технології програмно-конфігурованого радіо (SDR), який дозволить закріпити особливості формування (завадостійкого кодування, перемеження, модуляції, підсилення, перетворення частоти тощо), передавання, прийому (демодуляції, деперемеження, декодування тощо) сигналів цифрового телевізійного мовлення.

Література

1. Гельгор А.Л., Попов Е.А.Система цифрового телевизионного вещания стандарта DVB-T: Учеб. пособие. – СПб.: Изд-во Политехн. ун-та, 2010. – 207 с.
2. Digital Television Satellite, Cable, Terrestrial, IPTV, Mobile TV in the DVB Framework. Third Edition.
3. Стандарт DVB-S. Система цифрового ТВ вещания опис [Електроний ресурс**]:** база даних- Режим доступу: http://www.konturm.ru/tech.php?id=dvbs
4. IPTV vs. OTT [Електронний ресурс]. Режим доступу до ресурсу: https://nettech.ua/news/iptv-vs-ott-sdelayte-svoy-vibor
5. [Електронний ресурс]. Режим доступу: https://deps.ua/ua/knowegable-base/articles/9689.html
6. Палагін В. В. Основи телебачення : посібник для студентів напряму підготовки 6.050901 "Радіотехніка" [Електронний ресурс] / Авт.-укл. В. В. Палагін, А. В. Гончаров ; за ред. Ю. Г. Леги ; М-во освіти і науки України, Черкас. держ. технол. ун-т. – Черкаси : ЧДТУ, 2010. – 144 с.

УДК 004.738.5:621.39.072

ПРОБЛЕМИ ПРОЕКТУВАННЯ АРХІТЕКТУРИ БЕЗДРОТОВОЇ СЕНСОРНОЇ МЕРЕЖІ

[1]Гуйда О.Г., [1]Омецинська Н.В., [2]Новіков В.І., [2]Гетьман О.В.
[1]*Навчально-науковий інститут муніципального управління та міського господарства Таврійського національного університету імені В. І. Вернадського, Україна*
[2]*Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна*
E-mail: Guydasg@ukr.net, novikov1967@ukr.net,

PROBLEMS OF DESIGNING ARCHITECTURE FOR WIRELESS SENSOR NETWORK

The article discusses the importance of designing an effective architecture for wireless sensor networks that can be used for data collection in various fields such as environmental monitoring or medical diagnostics. The article focuses on key issues that arise when designing such a network. The authors examine each of the problems in detail and propose possible solutions to address them.

Вибір та проектування архітектури бездротових сенсорних мереж потребує попереднього аналізу і вирішення проблем, які виникають при проектуванні бездротових сенсорних мереж. До таких досліджують питання вибору оптимального протоколу передачі даних, забезпечення енергоефективності, маршрутизації даних та інші технічні проблеми, пов'язані з проектуванням таких мереж.

До основних ключових проблемах, що виникають при проектуванні такої мережі відносяться проблеми з енергопостачанням, синхронізацією годинників та локалізацією сенсорів у мережі, дизайном обладнання та собівартістю продукції та інше. Розглянемо більш детально основні технічні проблеми, пов'язані з проектуванням таких мереж.

Споживання енергії. У WSN енергоспоживання є однією з головних проблем. В якості джерела енергії використовується акумулятор, оснащений сенсорними вузлами. Сенсорна мережа влаштована в небезпечних ситуаціях, тому в іншому випадку замінити акумулятори стає складно. Споживання енергії в основному залежить від операцій сенсорних вузлів, таких як зв’язок, зондування та обробка даних. Під час спілкування споживання енергії дуже велике. Таким чином, споживання енергії можна уникнути на кожному рівні, використовуючи ефективні протоколи маршрутизації [1].

Локалізація. Для роботи мережі основною, а також критичною проблемою є локалізація датчика. Таким чином, сенсорні вузли розташовані в спеціальному порядку, щоб вони не знали про своє місцезнаходження. Складність визначення фізичного розташування датчика після того, як вони розташовані, відома як локалізація. Цю проблему можна вирішити за допомогою GPS, вузлів-маяків, локалізації на основі близькості [2].

Покриття. Сенсорні вузли в бездротовій сенсорній мережі використовують

алгоритм покриття для виявлення даних, а також передають їх на приймач через алгоритм маршрутизації. Щоб охопити всю мережу, необхідно вибрати сенсорні вузли. Рекомендуються такі ефективні методи, як алгоритми шляху найменшого та найвищого впливу, а також протокол проектування покриття [3].

Синхронізація годинників. У WSN синхронізація годин є серйозною послугою. Основна функція цієї синхронізації полягає в тому, щоб запропонувати звичайний часовий масштаб для вузлів локальних годинників у сенсорних мережах. Ці годинники повинні бути синхронізовані в деяких програмах, таких як моніторинг і відстеження [3].

Обчислення. Обчислення можна визначити як суму даних, яка продовжується через кожен вузол. Основна проблема в обчисленнях полягає в тому, що вони повинні зменшити використання ресурсів. Якщо тривалість життя базової станції більш небезпечна, то обробка даних буде завершена на кожному вузлі перед передачею даних на базову станцію. На кожному вузлі, якщо у нас є певні ресурси, тоді все обчислення має виконуватися на приймачі.

Вартість виробництва. У WSN організована велика кількість сенсорних вузлів. Отже, якщо ціна одного вузла дуже висока, загальна ціна мережі також буде високою. Зрештою, ціна кожного сенсорного вузла повинна бути меншою. Таким чином, ціна кожного сенсорного вузла в бездротовій сенсорній мережі є складною проблемою.

Дизайн обладнання. При розробці апаратного забезпечення будь-якої сенсорної мережі, наприклад керування живленням, мікроконтролер і комунікаційний блок мають бути енергоефективними. Його дизайн може бути виконаний таким чином, що він використовує низьку енергію.

Якість обслуговування. Якість обслуговування або QoS - це не що інше, як дані повинні бути розподілені в часі. Тому що деякі додатки на основі датчиків у реальному часі в основному залежать від часу. Отже, якщо дані не розподіляються вчасно до одержувача, вони стануть марними. У WSN існують різні типи проблем із QoS, наприклад топологія мережі, яка може часто змінюватися, а також доступний стан інформації, що використовується для маршрутизації, може бути неточним.

Структура бездротової сенсорної мережі. Структура WSN в основному складається з різних топологій, які використовуються для мереж радіозв'язку, таких як зірка, сітка та гібридна зірка. Ці топології коротко обговорюються нижче.

Зоряна мережа. Комунікаційна топологія типу зіркової мережі використовується скрізь, де тільки базова станція може передати або отримати повідомлення до віддалених вузлів. Існує кілька доступних вузлів, яким заборонено передавати повідомлення один одному. Переваги цієї мережі в основному полягають у простоті, здатній звести до мінімуму споживання енергії віддалених вузлів.

Це також дозволяє здійснювати зв'язок із меншою затримкою між базовою станцією та віддаленим вузлом. Основним недоліком цієї мережі є те, що базова станція повинна бути в зоні дії радіо для всіх окремих вузлів. Він не є надійним, як інші мережі, оскільки він залежить від одного вузла, який обслуговує мережу [4].

Mesh мережа. Цей тип мережі дозволяє передавати дані від одного вузла до

іншого в межах мережі, яка знаходиться в зоні дії радіопередачі. Якщо вузлу потрібно передати повідомлення іншому вузлу, який знаходиться поза зоною радіозв'язку, він може використовувати вузол як проміжний зв'язок, щоб надіслати повідомлення бажаному вузлу.

Основною перевагою сітчастої мережі є масштабованість, а також надмірність. Коли окремий вузол припиняє працювати, віддалений вузол може спілкуватися з будь-яким іншим типом вузла в межах діапазону, а потім пересилає повідомлення до бажаного місця. Крім того, діапазон мережі не обмежується автоматично через діапазон між окремими вузлами; його можна розширити, просто додавши кілька вузлів до системи.

Основним недоліком такого типу мережі є використання потужності для мережевих вузлів, які здійснюють зв'язок, наприклад багатохопове, зазвичай вище, ніж інші вузли, які не мають такої здатності часто обмежувати термін служби батареї. Більше того, коли кількість стрибків зв'язку збільшується до пункту призначення, час, витрачений на надсилання повідомлення, також збільшуватиметься, особливо якщо низька потужність процесу вузлів є необхідністю [5].

Hybrid Star – Mesh Network. Гібрид між двома мережами, як-от зірка та сітка, забезпечує потужну та гнучку комунікаційну мережу, зберігаючи при цьому мінімальне енергоспоживання бездротових сенсорних вузлів. У такій топології мережі сенсорні вузли з меншою потужністю не можуть передавати повідомлення. Це дозволяє мінімально використовувати електроенергію для обслуговування.

Але інші мережеві вузли мають можливість передавати повідомлення від одного вузла до іншого в мережі. Зазвичай вузли з багатопрохідною ємністю мають високу потужність і часто підключаються до мережі. Це реалізована топологія через майбутню стандартну сітчасту мережу під назвою ZigBee.[6]

Література

1. Пономаренко С.О., Тачиніна О.М., Лисенко О.І., Кисельов В.Б., Гуйда О.Г. Модель національної аерокосмічної системи розгортання глобальної сенсорної мережі. Вчені записки Таврійського національного університету ім. В. І. Вернадського", серія "Технічні науки": зб. наук. праць. Видавничий дім «Гельветика» Том 31 (70) № 6 2020 Частина 1. с. 21-26.
2. Akyildiz I.F. Wireless Sensor Networks /I.F. Akyildiz// Tutorial at IEEE INFOCOM. 2005. March 14.
3. Теорія оптимальних розгалужених траєкторій: монографія / О. І. Лисенко, О. М. Тачиніна, С. О. Пономаренко, О. Г. Гуйда. К: КПІ ім. Ігоря Сікорського., 7БЦ, 2023. 260 с.
4. K. Romer, Time synchronization in ad hoc networks, in Proceedings of ACM Symposium on Mobile Ad Hoc Networking and Computing,pp. 173–182. ACM, 2001.
5. J.R.Vig, Introduction to quartz frequency standards, Technical Report SLCETTR- 92-1, Army Research Laboratory Electronics and Power Sources Directorate, 1992.
6. K.-L. Noh and E. Serpedin, Pairwise broadcast synchronization for wireless sensor networks, in Proceedings of the IEEE International Workshop: From Theory To Practice in Wireless Sensor Networks, pp. 1–6. IEEE, 2007.

УДК 39.072

МЕТОДИ ЕНЕРГОЗБЕРЕЖЕННЯ НА ОСНОВІ ЕНЕРГОЕФЕКТИВНОЇ КЛАСТЕРИЗАЦІЇ ДЛЯ WSN

[1]Тачиніна О.М., [2]Гуйда О.Г., [3]Явіся В.С., [3]Гетьман О.В.

[1]Факультет аеронавігації, електроніки та телекомунікацій

Національний авіаційний університет, Україна

[2]Навчально-науковий інститут муніципального управління та міського господарства Таврійського національного університету імені В. І. Вернадського, Україна

[3]Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: Guydasg@ukr.net, tachinina5@gmail.com, yavisya_v@bigmir.net

METHODS OF ENERGY SAVING BASED ON ENERGY-EFFICIENT CLUSTERING FOR WSN

The article discusses methods of energy saving based on energy-efficient clustering for wireless sensor networks. The article provides an overview of several methods that can be used for efficient energy management in WSNs.

Методи енергозбереження є одним з головних напрямків розвитку бездротових сенсорних мереж (WSN). З метою забезпечення оптимальної роботи WSN, дослідники працюють над розробкою ефективних методів енергозбереження. Один з таких методів - енергоефективна кластеризація, яка забезпечує збільшення енергоефективності WSN [1].

У WSN, сенсорні вузли звичайно працюють з батарейним живленням. Це означає, що обмежені ресурси енергії, які потрібно ефективно використовувати, щоб продовжувати роботу мережі протягом тривалого часу. Є кілька способів енергозбереження, таких як керування

енергоспоживанням, регулювання потоку даних, маршрутизація та кластеризація [2].

Енергоефективна кластеризація - це процес групування сенсорних вузлів у кластери, які мають вищу енергоефективність. Кожен кластер має свого керівника, який забезпечує збір даних та їх передачу до базової станції. Це дозволяє зменшити кількість передаваних повідомлень та збільшити час роботи мережі за рахунок зменшення енергоспоживання сенсорних вузлів [3].

Є кілька методів енергоефективної кластеризації. Один з них - Low Energy Adaptive Clustering Hierarchy (LEACH) [4], що використовується для WSN з рівномірним розподілом сенсорних вузлів. LEACH забезпечує рівномірне розподілення енергії між сенсорними вузлами, що зменшує кількість вузлів, які переривають свою роботу через виснаження енергії батареї.

Інший метод - Stable Election Protocol (SEP) [5], який застосовується для WSN з нерівномірним розподілом сенсорних вузлів. SEP забезпечує вибір керівників кластерів, які мають більшу залишкову енергію. Це дозволяє зменшити кількість повідомлень, які передаються від сенсорних вузлів до базової станції, тим самим зберігаючи енергію в батареї сенсорних вузлів.

Інші методи енергозбереження на основі енергоефективної кластеризації включають Multi-Hop Routing Protocol (MRP), Threshold Sensitive Energy Efficient Network Protocol (TEEN) та Distributed Energy Efficient Clustering (DEEC).

У більшості досліджень, що використовують метод енергоефективної кластеризації, використовується моделювання та симуляція в програмному забезпеченні. Однак, деякі дослідження використовують реальні WSN для перевірки ефективності запропонованих методів [9].

Методи енергозбереження на основі енергоефективної кластеризації для WSN дуже важливі для забезпечення довготривалої роботи мережі та зменшення затрат на заміну батарей. Існує багато методів, які можуть бути

використані для WSN в залежності від сценарію використання. Однак, дослідження цих методів дозволить визначити найбільш ефективний метод для конкретної WSN. Застосування методів енергозбереження на основі енергоефективної кластеризації є важливим кроком у покращенні довговічності та ефективності WSN, що в свою чергу підвищує їх прикладну цінність.

Отже, енергоефективна кластеризація є ефективним методом енергозбереження для WSN. Методи, такі як LEACH, SEP, MRP, TEEN та DEEC, є ефективними в різних сценаріях роботи WSN. Дослідження цих методів може допомогти визначити найкращий метод для конкретного застосування WSN.

Література

1. Теорія оптимальних розгалужених траєкторій: монографія / О. І. Лисенко, О. М. Тачиніна, С. О. Пономаренко, О. Г. Гуйда. К: КПІ ім. Ігоря Сікорського., 7БЦ, 2023, 260 с.
2. Y. Wang, X. Cheng, J. Chen, and X. Xu, "Research on Energy Saving Techniques in Wireless Sensor Networks," in 2016 IEEE 2nd Information Technology and Mechatronics Engineering Conference (ITOEC), 2016, pp. 9-12.
3. W. Guo, Y. Wang, and L. Yang, "An Energy-Efficient Clustering Routing Algorithm for Wireless Sensor Networks Based on LEACH," in 2018 International Conference on Computer, Information and Telecommunication Systems (CITS), 2018, pp. 1-5.
4. Z. Ma, F. Li, Y. Li, and H. Li, "An Energy Efficient Clustering Algorithm Based on LEACH for Wireless Sensor Networks," in 2015 International Conference on Computing, Communication and Security (ICCCS), 2015, pp. 1-4.
5. A. Manjeshwar and D. P. Agrawal, "TEEN: A Protocol for Enhanced Efficiency in Wireless Sensor Networks," in 2001 International Parallel and Distributed Processing Symposium (IPDPS), 2001, pp. 2009-2015.
6. S. Lin, Y. Hu, and K. Yang, "Energy Efficient Clustering Routing Algorithm for Wireless Sensor Networks," in 2016 International Conference on Robotics, Control and Automation Engineering (RCAE), 2016, pp. 75-78.

УДК 621.382

АНАЛІЗ НАПРЯМКІВ ПОБУДОВИ РАЦІОНАЛЬНОЇ АРХІТЕКТУРИ МЕРЕЖІ 5G НА ОСНОВІ ІСНУЮЧИХ 4G МЕРЕЖ

Правило В.В.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: v.v.pravylo@ukr.net

ANALYSIS OF DIRECTIONS FOR BUILDING A RATIONAL 5G NETWORK ARCHITECTURE BASED ON EXISTING 4G NETWORKS

The migration scenario from LTE to 5G networks is presented. Options for choosing the level of integration are offered.

Сценарії міграції від LTE до 5G.

Найбільш затребуваною стратегією розгортання 5G для операторів зв'язку, ймовірно, буде довгострокове співіснування мереж 4-го і 5-го покоління з максимальним повторним використанням інфраструктури, вузлів і елементів мережі. Це дозволить операторам модернізувати свої мережі не революційно, а прогресивно (еволюційно), з одного боку, зберігаючи інвестиції в будівництво LTE-мереж і широку зону радіопокриття мереж LTE, з іншого – надавати клієнтам нові послуги на основі 5G в областях, де ці послуги користуються попитом.

Вибір рівня інтеграції.

Рівень, на якому стикаються стеки протоколів LTE і 5G, визначається як рівень інтеграції. Цей рівень має інтерфейс для нижчих рівнів, які відносяться до різних технологій радіодоступу, але пропонує однакові послуги для рівня інтеграції. Останній буде доставляти пакети з верхніх шарів до різних RAT, і збирати трафік, що надходить з різних нижніх шарів.

Варіанти вибору рівня інтеграції:

Спільний рівень **PHY**: це рішення теоретично може бути життєздатним, так як OFDM або один з його варіантів, як очікується, буде основою для архітектури фізичного рівня 5G. Однак 5G використовуватиме дуже різні структури кадрів і

нумерологія для різних цілей. Тому інтеграція LTE і 5G на рівні PHY є дуже складним завданням, і переваги будуть обмежені.

Більше того, використання загального рівня PHY обмежує можливість змін стеку верхніх шарів, щоб адаптувати його до вимог 5G. Нарешті, операції на Рівні PHY в цьому випадку повинні бути сильно синхронізовані, і це запобігає нерозміщеному розгортанню eNB для різних RAT;

Спільний рівень **MAC**: інтеграція на рівні MAC може забезпечити високий рівень координації. Можливим варіантом агрегації MAC є агрегація

несучих, яка вже стандартизована для LTE. На цьому рівні можливо координувати планування ресурсів для різних RAT, виконувати HARQ на різних носіях та уникати труднощів передачі контексту між RLC та PDCP, оскільки для кожного носія буде по одній копії обох. Однак операції рівня MAC синхронізовані, що дозволяє розгортання лише спільно розташованих RAT. Більше того, LTE і 5G можуть розроблятися з різними дуплексними рішеннями та різними схемами розподілу часу та частоти. Тому, хоча потенційні переваги дуже привабливі, інтеграція на MAC обмежує можливості проектування управління доступом до 5G, на відміну від LTE, не допускає абсолютно нового дизайну, який враховує особливості комунікацій mmWave;

Спільний рівень **RLC**: цей вибір має деякі обмеження, що здатні запобігти розгортанню без спільного розміщення. Дійсно, рівень RLC приймає з інструкцій планувальника рівня MAC укази щодо можливостей передачі, тобто скільки байтів доступно для передачі протягом наступного інтервалу часу. Цей зв'язок не може підлягати додатковим затримкам зв'язку MAC-RLC між віддаленими точками розміщення. Крім того, сегментація і повторне складання працюватиме тільки при наявності загального планувальника. Врешті, основною перевагою інтеграції на стеці RLC є наявність однієї передачі і, для AM RLC, буфера повторної передачі, що здатне покращити координацію між двома RAT;

Загальний рівень **PDCP**: рівень PDCP не має жорстких вимог до синхронізації і тому може бути чудовим кандидатом як рівень інтеграції, коли бажаний підхід не пов’язаний із спільним розташуванням. Інтеграція на рівні PDCP дозволяє створювати з чистого аркуша рівні PHY, MAC і RLC, щоб їх можна було адаптувати до нових вимог мереж 5G.

Для реалізації цієї стратегії 3GPP запропонував кілька можливих сценаріїв (або варіантів) впровадження 4G (LTE) і 5G (NR). Всі варіанти діляться на дві основні групи:

1. Standalone (SA) - передбачають використання тільки однієї технології радіодоступу (LTE або NR - New Radio);

2. Non-Standalone (NSA) - використання і LTE і NR, що спрощує розгортання мереж 5G на початковому етапі.

Неавтономне розгортання 5G вимагає оновлення базових станцій 4G-LTE до eLTE (або розширеного LTE), щоб підтримувати розширені функції базової станції 5G (gNb). Стандартизація цього сценарію (в рамках випуску 15 3GPP) була завершена в січні 2018 року.

Важливим аспектом для реалізації неавтономних опцій є концепція подвійного підключення, визначена 3GPP у випуску 12, яка передбачає підключення терміналів користувача (UE) у стані RRC_CONNECTED до двох базових станцій одночасно (Master eNb і Secondary eNb). Ключова відмінність між подвійним підключенням та агрегацією частот полягає в тому, що він підключається до двох різних базових станцій, підключених

через інтерфейс X2, і, як правило, розташовані на різних сайтах.

При цьому можливі дві схеми реалізації:

1. split bearer - в цій схемі на PDCP рівні потік призначених для користувача даних (user plane) віртуального каналу розщеплюється на два підпотоків в напрямку Master eNb і Secondary eNb відповідно;

2. switch bearer - в цій схемі потік призначених для користувача даних (user plane) може комутуватися або в напрямку Master eNb, або в напрямку Secondary eNb (без агрегації).

Реалізація Non-Standalone накладає додаткові вимоги до складності користувацьких терміналів (UE), включаючи одночасну роботу двох модемів, збільшення розміру буфера та додаткове навантаження на ресурси процесора рівня PDCP для відновлення порядку пакетів (у режимі MCG split bearer).

Вибір сценарію міграції.

Зараз у багатьох розвинених країнах вже є покриття 4G по всій або майже по всій країні. В Україні ситуація інша, оскільки великі території залишаються неохопленими навіть мережами третього покоління, але на це є як технічні так і інші об’єктивні причини. Проте всі великі міста мають покриття 4G від великих українських операторів мобільного зв’язку, а великі міста є першими кандидатами на впровадження нових мобільних технологій п’ятого покоління, оскільки в них є великий натовп людей, є потреба у вищій швидкості мобільного інтернету та більша пропускна здатність, можливість одночасно надавати послуги великій кількості людей і підключати величезну кількість різних пристроїв, є бажання розвивати Інтернет речей для реалізації ідей «розумного» міста, автоматизувати багато процесів. Першими кандидатами на покриття 5G є стадіони, великі торгові центри тощо.

Враховуючи наявність повністю розгорнутих і функціонуючих мереж четвертого покоління, найкращим рішенням було б використовувати їх на ранніх етапах впровадження нової технології 5G. У будь-якому випадку цим технологіям доведеться співіснувати дуже довго, тому потрібно зробити їх взаємодію максимально ефективною і непомітною для звичайного користувача.

Поступове впровадження дозволить операторам оновлювати свої мережі поступово, без поспіху, зберігаючи при цьому широке покриття 4G, пропонуючи клієнтам, які зацікавлені в нових можливостях, які відкриваються з технологіями наступного покоління.

Тому використання сценарію Non-Standalone (NSA) є найбільш оптимальним для операторів та їх клієнтів.

Література

1. Jackson, Cyrus, The 5G Network Architecture: A Guide That Covers Everything About The 5G Technology , ISBN 13: 9798644075591.
2. Ge Xiaohu, Zhang Wuxiong. 5G Green Mobile Communication Networks.
3. Launay Frédéric, Perez André. LTE Advanced Pro: Towards the 5G Mobile Network.

УДК 621.39

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ MPTCP ДЛЯ ПІДВИЩЕННЯ ЖИВУЧОСТІ WIFI КАНАЛІВ УПРАВЛІННЯ БПЛА В УМОВАХ ВПЛИВУ НАВМИСНИХ ТА НЕНАВМИСНИХ ЗАВАД

Гетьман О.В., Кайденко М.М., Роскошний Д.В.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: kkk610@ukr.net

USING MPTCP TECHNOLOGY TO INCREASE THE SURVIVABILITY OF WIFI UAV CONTROL CHANNELS UNDER THE INFLUENCE OF INTENTIONAL AND UNINTENTIONAL INTERFERENCE

This paper proposes the use of MPTCP technology to create UAV control and communication channels. Such control channels will be protected from the influence of various kinds of attacks on the UAV. Features of technology and flow control mechanisms in MPTCP are considered . The proposed solution was tested in laboratory conditions on a test stand using the appropriate software.

В останні роки безпілотні літальні апарати (БПЛА) все більше використовуються для різних застосувань як у військових цілях, так і в цивільних. Однак все більше поширення застосування БПЛА збільшує й проблеми безпеки. Особливо це стосується вразливості каналів управління БПЛА до впливу різноманітних типів атак на них. В роботах [1-4] було запропоновано комплекс рішень по підвищенню стійкості каналів управління та зв'язку БПЛА до впливу на них навмисних та ненавмисних завад, які базуються на побудові каналів управління з використанням двох каналів зв'язку в двох діапазонах частот.

Існує цілий клас безпілотних літальних апаратів, які використовують технології WiFi для організації каналів управління, телеметрії та передачі даних. Для цих БПЛА також можливе використання запропонованих в [1-4] рішень з одночасною роботою в двох діапазонах частот - 2,4 ГГц та 5 ГГц. В таких безпілотних апаратах для здешевлення використовуються стандартні WiFi модулі та програмне забезпечення управління на базі Embedded Linux. Однак застосування високоефективних алгоритмів протидії впливу навмисних завад має істотні недоліки в силу існуючого обмеження на кількість доступних параметрів каналу зв’язку, якими визначається стан каналу. По суті використання стандартних WiFi модулів, що побудовані на недорогих чіпсетах, одночасно з використанням стандартних драйверів Linux обмежує можливості цих алгоритмів внаслідок невеликої кількості доступних параметрів для аналізу стану каналу зв'язку [5]. Так, доступними параметрами про стан каналу для інтерфейсу Interface wlp2s0, який виводиться командою iw dev після введення команди iw dev wlp2s0 link є: рівень прийнятого сигналу та швидкість передачі в каналі. Введення команди iw dev wlp2s0 station dump дозволяє додатково визначити середній рівень прийнятого сигналу, кількість повторних запитів на передачу пакетів: та кількість втрачених пакетів при передачі. Цих параметрів достатньо буде лише для того, щоб визначити характеристику прийнятого сигналу за рівнем

прийнятого сигналу, а якість сигналу визначається тільки за кількістю втрачених пакетів. Таким чином використання обмеженої кількості параметрів буде достатнім лише для протидії впливу завадам глушення каналу. Для протидії впливу іншим видам завад потрібні інші алгоритмічні рішення. Найбільш ефективним є використання технології багатомаршрутного TCP (Multipath TCP).

Технологія MPTCP — одне з найважливіших розширень TCP, що дозволяє використання кількох шляхів передачі для TCP-з'єднання. У MPTCP кінцеві хости передають дані з кількох підпотоків TCP одночасно по одному з'єднанню. MPTCP може досить ефективно використовувати ресурси смуги пропускання для підвищення ефективності передачі. Також ця технологія забезпечує стійкість організованого таким чином каналу зв'язку завдяки багатоканальній передачі даних. У додатках та рішеннях, де важлива швидкість передачі даних та надійність, MPTCP може бути найбільш перспективним підходом до вирішення цих проблем у випадку, коли інші методи є недоступними.

MPTCP розроблено з урахуванням таких моментів: підвищення пропускної спроможності; не створення негативного впливу на звичайний TCP; балансування навантаження і підвищення відмовостійкості за рахунок зміщення потоків з перевантаженого, або несправного шляху, на найменший перевантажений шлях.

Застосуванню MPTCP для організації зв'язку в рухомих засобах присвячено велику кількість досліджень, при цьому велика увага присвячується саме автомобільним мережам. Відзначається, що вибір правильних шляхів передачі дуже важливий. Дослідження щодо багатошляхової маршрутизації *[6]* проводилися для забезпечення ефективності і надійності шляхів передачі. Закордонні дослідники також проводять дослідження, відносно застосовання MPTCP технологій в безпілотних літальних апаратах. В роботі [7] було запропоновано безпілотну літальну систему, яка використовує кілька взаємодіючих БПЛА.

MPTCP має два важливі механізми керування потоком, а саме контроль перевантаження і планувальник пакетів. Контроль перевантаження відповідає за контроль викликаного навантаження на мережу щоб уникнути перевантаження мережі. Традиційний TCP з одним маршрутом використовує алгоритм уникнення перевантажень, який включає схему повільного запуску та схему адитивного збільшення/мультиплікативного зменшення (AIMD — additive increase/multiplicative decrease).

Механізм контролю перевантаження MPTCP був розроблений і стандартизований [8]. З іншого боку, планувальник відповідає за розповсюдження даних кількома шляхами. Належний планувальник може покращити хорошу пропускну здатність (пропускна здатність на рівні програми), або забезпечити високу надійність передачі інформації навіть в умовах впливу на канал навмисних завад. Однак, на відміну від контролю перевантаження MPTCP, планувальник ще не стандартизований. Найбільш часто використовуваними планувальниками є циклічний планувальник (RR - round robin) і найкоротший згладжений (RTT -Round Trip Time), чи (SRTT - Shortest Smoothed RTT). Планувальник реалізації MPTCP ядра Linux [9] базується на SRTT. Останніми роками було проведено багато досліджень щодо контролю перевантажень і планувальника MPTCP, є також деякі

дослідження, які поєднують контроль перевантаження MPTCP і планувальник разом для покращення продуктивності та якості передачі.

Для каналу зв'язку та управління БПЛА, який реалізується на базі двох модулів WiFi для діапазонів частот 2,4 та 5 ГГц, що працюють під управлінням операційної системи на базі Linux один з варіантів MPTCP може бути реалізований як в розроблений в відкритому проекті [10].

Процес створення та реалізації MPTCP було перевірено та реалізовано в лабораторних умовах з використанням тестового стенду. Для перевірки було встановлено відповідну версії Linux, яка використовується в якості Embedded Linux, версію MultiPath TCP. Встановлена версія Linux відповідала також версії для Raspberry PI, яка дуже часто використовується в малогабаритних БПЛА. В якості робочої станції в стенді було використано ноутбук, в якому було встановлено два модулі WiFi для діапазонів частот 2,4 та 5 ГГц.

Література

1. 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
2. M. M. Kaidenko and S. O. Kravchuk, "Anti-Jamming System for Small Unmanned Aerial Vehicles," 2021 IEEE 6th International Conference on Actual Problems of Unmanned Aerial Vehicles Development (APUAVD), 2021, pp. 1-4, doi: 10.1109/APUAVD53804.2021.9615403.
3. Mykola M. Kaidenko, Serhii O. Kravchuk "PROTECTION AGAINST THE EFFECT OF DIFFERENT CLASSES OF ATTACKS ON UAV CONTROL CHANNELS" Information and Telecommunication Sciences, No.1, pp. 35-43, 2022. https://doi.org/10.20535/2411-2976.12022.35-43
4. Kaidenko, M., Kravchuk, S. (2023). Principles of Constructing Communication and Control Systems Protected from the Effects of Jamming Attacks for Small-Sized Unmanned Aerial Vehicles. In: Ilchenko, M., Uryvsky, L., Globa, L. (eds) Progress in Advanced Information and Communication Technology and Systems. MCiT 2021. Lecture Notes in Networks and Systems, vol 548. Springer, Cham. https://doi.org/10.1007/978-3-031-16368-5_20
5. Network configuration - Режим доступу: https://wiki.archlinux.org/title/Network_configuration
6. Zhang, T.G.; Zhao, S.; Cheng, B. Multipath Routing and MPTCP-Based Dara Delivery over MANETs. IEEE Access 2020, 8, 32652–32673.
7 Chirwa, R.M.N.; Lauf, A.P. Performance improvement of transmission in Unmanned Aerial Systems using multipath TCP. In Proceeding of the 2014 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), Noida, India, 15–17 December 2014; pp. 19–24.
8. Raiciu, C.; Handley, M.; Wischik, D. Coupled Congestion Control for Multipath Transport Protocols; RFC6356; IETF: Fremont, CA, USA, 2011.
9. Multipath TCP in the Linux Kernel. Available online: https://www.multipath-tcp.org/ (accessed on 3 October 2020).
10. MultiPath TCP - Linux Kernel implementation - Режим доступу: https://multipath-tcp.org/pmwiki.php/Main/HomePage

УДК 621.39

ВИКОРИСТАННЯ СИСТЕМ-НА-КРИСТАЛІ РАДІОЧАСТОТНОГО ЗАСТОСУВАННЯ ПРИ РОЗРОБЦІ SDR СИСТЕМ

Гетьман О.В., Кайденко М.М., Роскошний Д.В.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: ккк610@ukrl.net

USING RF SYSTEM-ON-CHIP IN THE DEVELOPMENT OF SDR SYSTEMS

The concept of SDR and the three primary architectures for implementing SDR has considered. The RFSoC devices are able to perform many of required functions in MIMO systems, beamforming, radio standards for mobile networks.

Програмно визначені радіосистеми (SDR) - це системи радіозв'язку, де компоненти, які традиційно впроваджуються в апаратне забезпечення (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.[1]

Основна ідея використання пристроїв SDR полягає в тому, що одним або декількома аспектами функціональності радіопристрою можна керувати за допомогою програмного забезпечення.

Сьогодні не існує єдиної остаточної архітектури для SDR. Для створення систем SDR можна використовувати кілька різних варіантів побудови пристроїв, деякі з них наведено на рис 1 (а – реалізація на трьох пристроях, б – на двох, в – одночіпова реалізація).

Основними апаратними елементами SDR є:

• Антена(и)

• Фронтенд, що виконує функції формування сигналу, (включаючи підсилювачі та фільтри), аналогового змішування та перетворення даних ха допомогою АЦП та ЦАП)

• Платформа(и) обробки

Вибір апаратних компонентів у SDR зазвичай залежить від функціональних критеріїв (таких параметрів, як несуча радіочастота, швидкості передачі даних і параметрів, що витікають з них), продуктивності та обмежень щодо вартості.

Іншим важливим фактором є кількість підтримуваних радіоканалів передачі та прийому.

Хоча можливо реалізувати SDR, використовуючи окремі компоненти для реалізації кожного з перерахованих вище елементів, все частіше

з'являються інтегровані продукти, які поєднують деякі з вищезазначених функцій.

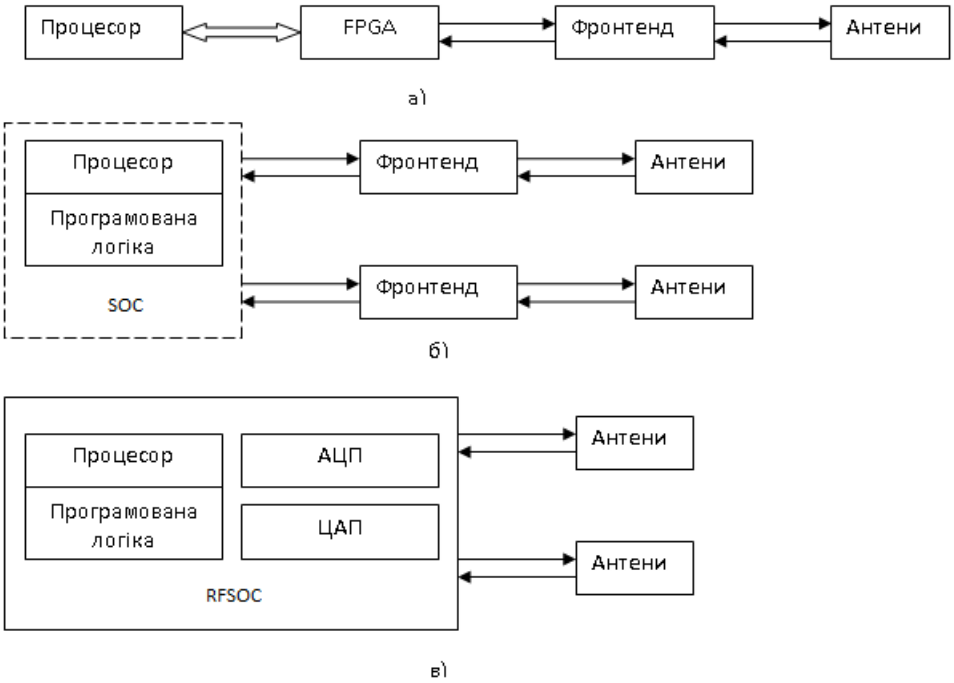


Рисунок 1. Варіанти побудови пристроїв SDR.

Одним з таких високоінтегрованих продуктів є новітні апаратні платформи – системи на кристалі для радіочастотних застосувань - RFSoC, які поєднують в собі конвертери даних із платформою обробки.

Більшість пристроїв RFSoC підтримують до 16 каналів передачі та прийому. Інтеграція такої великої кількості каналів на одному чіпі є потужним засобом для побудови різноманітних радіосистем. Багатоканальні можливості RFSoC можна використати для реалізації: систем із кількома входами та кількома виходами (MIMO), формування променю та радіосистем, які підтримують кілька різних стандартів одночасно.

MIMO — це техніка бездротового зв'язку, яка поширюється на конфігурацію Single Input Single Output (SISO), тобто один передавач і приймач, замість цього використовується кілька передавачів і приймачів.

Техніка MIMO використовує просторове рознесення, оскільки кожна з передавальних та приймальних антен займає різне положення в просторі, і тому компоненти сигналу проходять різні фізичні шляхи через радіоканал. Набори передавальних і приймальних антен зазвичай розташовуються в лінійних або двовимірних масивах, при цьому найпростіші системи MIMO включають два передавача і два приймача. Існує концепція «Massive MIMO», яка використовує значно більше антен. Системи Massive MIMO можуть використовувати до 64 антен [2].

Чим більша кількість антен, тим більший потенціал для використання просторового рознесення та, таким чином, покращення пропускної здатності через бездротове з'єднання.

Формування променю є ще одним прикладом системи, де потрібно

кілька антен. Цю техніку використовують на передавачі, щоб електронно керувати напрямком випромінюваної енергії, і на приймачі, щоб електронно керувати чутливістю в бажаному напрямку. Також можна генерувати «нулі» в певних напрямках як засіб пом'якшення впливу перешкод.

Одна з головних переваг у цьому контексті полягає в тому, що напрямок променю можна динамічно змінювати за допомогою алгоритмів цифрової обробки без будь-якої необхідності фізично переміщувати антени. Подібно до MIMO, антени можна розташовувати в різних конфігураціях у фізичному просторі, і більша кількість антен передбачає більшу точність керування під час керування променем. Формування променю та MIMO також можна комбінувати, щоб направляти промені на конкретних абонентів у тривимірному просторі [3]. Ця техніка збільшує пропускну здатність стільникових мереж шляхом просторового повторного використання доступного радіоресурсу.

Як для додатків MIMO, так і для програм формування променю важливо, щоб канали були синхронізовані з однаковим опорним часом і частотою. У RFSoC це підтримується функцією Multi-Tile Synchronization, яка може синхронізувати канали в одному або на кількох пристроях [4], [5].

Крім систем з декількома антенами, багатоканальні властивості RFSoC також можна використовувати для підтримки кількох різних радіостандартів на одному чіпі. [6], [7]. Цей підхід можна порівняти з більш складною загальною системою або навіть реалізацією, яка вимагає кількох окремих пристроїв.

Література

1. Кайденко М.М., Роскошний Д.В. «Особливості застосування SYSTEM-ON-CHIP INTEL та XILINX при розробці SDR систем» // XV Міжнародна науково-технічна конференція "Перспективи телекомунікацій" ПТ-2021 Збірник матеріалів конференції.К.: КПІ ім. Ігоря Сікорського, 2021.– с.183 - 185
2. T. L. Marzetta, "Massive MIMO: An Introduction," Bell Labs Technical Journal, vol. 20, pp. 11-22, March 2015
3. M. N. Hamdy, "Beamformers Explained," Commscope white paper, 2020. Available: https://www.commscope.com/globalassets/digizuite/542044-beamformer-explained-wp-114491-en.pdf https://www.intel.ru/content/www/ru/ru/products/programmable/soc.html
4. AMD, "Zynq UltraScale+ RFSoC RF Data Converter v2.6 Gen 1/2/3 Product Guide", April 2022.Available: https://www.xilinx.com/content/dam/xilinx/support/documents/ip_documentation/usp_rf_data_converter/v2_6/ pg269-rf-data-converter.pdf
5. AMD, "Synchronization of Signal Processing in Multiple RF Data Converters Subsystems," XAPP1349 (v1.0), February 2022. Available: https://xilinx.eetrend.com/files/2022-03/wen_zhang_/100558157-244514-xapp1349-rfdc-subsystems.pdf
6. Microwave Journal, "AMD's Latest RFSoC Added to Evenstar O-RAN Reference Designs," 11th May 2022. Available: https://www.microwavejournal.com/articles/38122-amds-latest-rfsoc-added-to-evenstar-o-ran-reference-designs
7. S. S. Pereira, L. Almeida, A. S. R. Oliveira, N. B. Carvalho, and P. P. Monteiro, "Multi-band, Multi-technology Remote Unit (RU) Based on RFSoC", 50th European Microwave Conference, Utrecht, Netherlands, January 2021.

УДК 621.396.1

ВІДКРИТА АРХІТЕКТУРА DRONE ID ТА ПРОТОКОЛ ДИСТАНЦІЙНОЇ ІДЕНТИФІКАЦІЇ ДРОНІВ

Кравчук С.О.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail:sakravchuk@ukr.net

DRONE ID OPEN ARCHITECTURE AND REMOTE DRONE IDENTIFICATION PROTOCOL

This paper reviews a selection of open source projects used in drones, reviews open source systems for flight surveillance, including unmanned traffic management (UTM), flight control, flight safety and authorization, and mainly remote identification.

Загальновідомо, що програмне забезпечення (ПЗ) з відкритим вихідним кодом означає ПЗ, вихідний код якого є загальнодоступним. Це дозволяє перевіряти, модифікувати та покращувати програмне забезпечення. Програмне забезпечення з відкритим вихідним кодом зазвичай регулюється умовами ліцензування. Подібним чином апаратне забезпечення/виконання з відкритим вихідним кодом представляє собою апаратне забезпечення, дизайн/конструктив якого є загальнодоступним, що дозволяє на основі цього дизайну вивчати, змінювати, розповсюджувати та створювати нове апаратне забезпечення. Відкриті інтерфейси прикладного протоколу (API) дозволяють власному програмному забезпеченню спілкуватися з іншим програмним забезпеченням без доступу до вихідного коду [1].

Безпілотні літальні апарати (БПЛА) мають розвинену систему програмного забезпечення з відкритим кодом. Майже кожен аспект створення, польоту та навігації дрона (малого БПЛА) можна реалізувати за допомогою технологій з відкритим кодом.

Дрони можуть бути організовані за ієрархією рівнів зверху вниз: контроль за польотами; керування та контроль за дроном; симуляція; операційна система; апаратне забезпечення.

Управління польотами пов’язане з управлінням трафіком, дозволом на політ, підтвердженням безпеки та дистанційною ідентифікацією. Управління дроном стосується апаратного та програмного забезпечення, що використовується для польоту та керування дроном. Симуляція дрону стосується всіх аспектів його польоту та може включати аспекти керування траєкторією, моделі транспортних засобів, фізичні моделі, моделі погоди та візуалізацію. Що стосується безпроводової мережі дрону, симуляція може включати такі системи зв’язку, як LTE, діаграми спрямованості антен, моделі каналів і втрати на шляху. Апаратне забезпечення та операційні системи взаємодіють із програмним забезпеченням дрону з фізичним БПЛА. Для управління дронів, що працюють на відкритому устаткуванні, було розроблено спеціалізовані операційні системи з відкритим вихідним кодом.

В даній роботі розглядається вибірка проектів з відкритим кодом, які використовуються в дронах, розглядаються системи з відкритим вихідним кодом для спостереження за польотами, включаючи управління безпілотним рухом (UTM), управління польотами, безпека польотів і авторизація, а, головним чином, дистанційна ідентифікація.

Маленькі UA «малонаглядані», оскільки вони: зазвичай мають мале поперечний переріз радіолокації; видають шум, дуже помітний на близькій відстані, але його важко виявити на відстані, яку вони можуть швидко скоротити; зазвичай літають на малих висотах; мають високу маневреність, тому можуть літати під деревами і між будинками. Дрон може нести корисне навантаження, включаючи датчики, кібер- і кінетичну зброю, або може використовуватися як зброя, направляючи її в ціль. На них можуть літати неосвічені, недбалі чи злочинні оператори. Таким чином, основною функцією ідентифікаційною функцією є «Ідентифікація свого або чужого» (IFF, Identification Friend or Foe) для пом'якшення значної загрози, яку вони становлять. Інші програми можуть бути включені або полегшені за допомогою RID (Remote Identification and tracking). Зважайте на важливість ідентифікаторів у багатьох інтернет-протоколах і службах, наприклад, повні

доменні імена (FQDN), ідентифікатори транспортних протоколів, порти UDP та TCP, уніфіковані ідентифікатори ресурсів (URI), ідентифікатори відкритого ключа X.509, адреси електронної пошти, цифрові ідентифікатори об'єктів (DOI) та багато іншого, за що відповідає функція управління просторами IP-адрес IANA (Internet Assigned Numbers Authority).

Має місце також мережний RID в кількох варіантах. Дрон може мати постійне підключення до Інтернету, і в цьому випадку він може постійно отримувати інформацію RID безпосередньо через Інтернет. Дрон може мати переривчасте підключення до Інтернету, і в цьому випадку GCS (Ground Control Station) повинен отримати інформацію RID, коли сам дрон перебуває в автономному режимі. Дрон може не мати власного з’єднання з Інтернетом, але натомість мати іншу форму зв’язку з іншим вузлом, який може передавати інформацію RID в Інтернет. В цьому останньому випадку ретранслятором зазвичай буде GCS (який для виконання своїх функцій повинен знати, де знаходиться дрон, хоча збої в з’єднанні C2 (Command and Control) трапляються). Дрон може не мати засобів отримання інформації RID, у такому випадку GCS або інший доступний для оператора інтерфейс повинен отримати її. Це все може перешкоджати усуненню неоднозначності ідентифікатора, якщо кілька дронів працюють в одному об’ємі.

Література

1. Drone Security and the Mysterious Case of DJI’s DroneID / N. Schiller, M. Chlosta, M. Schloegel // Network and Distributed System Security (NDSS) Symposium 2023, 27 February - 3 March 2023, San Diego, CA, USA, ISBN 1-891562-83-5.

УДК 621.396.1

ТЕХНОЛОГІЇ ТА СИСТЕМИ ПРОТИДІЇ ЗАГРОЗАМ ВІД МАЛИХ ДРОНІВ

Кравчук С.О., Кравчук І.М.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail:sakravchuk@ukr.net

TECHNOLOGIES AND SYSTEMS FOR COUNTERING THREATS FROM SMALL DRONES

Technologies to counter drones (drone swarms) can have different purposes, but at the same time play an important role in ensuring security. All systems for countering drone threats can be divided into two broad categories: Monitoring Equipment and Countermeasures.

Технології протидії дронам (роям дронів) можуть мати різні призначення, але при цьому відігравати важливу роль у забезпеченні безпеки. У мирний час технології протидії дронам застосовуються для забезпечення безпеки повітряного простору навколо критично важливих об'єктів інфраструктури та великих заходів, таких як енергетичні вузли, спортивні ігри та музичні фестивалі, а також для захисту певних персон, приватних володінь та протидії проти будь-якої контрабанди в повітрі. У воєнний час (або в період терористичних атак) такі технології використовуються для захисту баз, складів, полігонів, військових кораблів, конвоїв та наземних підрозділів. Технології протидії дронам, для реалізації яких часто застосовуються неоднорідні сенсорні системи, у будь-якому своєму призначенні є складними багатоетапними процесами, що включають взаємодію між рядом окремих систем/об'єктів/сенсорів, а також між цими системами/об'єктами і оператором (людиною або штучним інтелектом) [1-3].

Усі системи опору загрозам дронів можна розділити на дві великі категорії: обладнання моніторингу та засоби протидії (Monitoring Equipment and Countermeasures).

Обладнання для моніторингу дронів може бути пасивним (простий огляд та прослуховування) або активним (випромінює сигнал та аналізує відбитий) і може виконувати такі функції: виявлення; класифікація та ідентифікація (розпізнавання); пошук та відстеження; оповіщення (якщо потрібно).

Більшість устаткування неспроможна виконувати одночасно всі перелічені вище функції, що знижує їх ефективність. У кращому випадку системи моніторингу повинні виявляти, ідентифікувати, визначати місцезнаходження і відстежувати дрон, що наближається. Залежно від типу системи, що використовується, сенсору, що виробляє початкове виявлення (наприклад, радіолокація), може знадобитися «перехресна передача» вторинним сенсорам, таким як оптичні матриці або електронні ідентифікаційні елементи, щоб підтвердити, що виявлений об'єкт, по суті, є дроном (а не птахом), а також визначити його точне місцезнаходження з відстеженням його переміщення. Вторинні сенсори також можуть служити для надання додаткової інформації про дрону, яка допоможе визначити його

намір. Наприклад, відеокамера може показати, чи дрон несе небезпечне навантаження – бомбу, озброєння.

Ґрунтуючись на інформації від усіх сенсорів системи моніторингу, оператор у дуже обмежений час має ухвалити рішення про те, як реагувати на виявлений дрон. Це не завжди може включати активацію системи протидії/захисту, особливо в мирний час.

Для перехоплення дрону застосовуються засоби протидії, що може призвести в залежності від техніки, що використовується, до різних наслідків. Наприклад, посадка дрону на землю (у разі глушіння чи спуфінгу), активація режиму «повернення додому», захоплення дрона (простими мережами), його повне чи часткове знищення.

Системи моніторингу дронів. Існують такі типи обладнання для моніторингу дронів: радіочастотні аналізатори (Radio Frequency (RF) Analyzers), акустичні датчики (мікрофони), оптичні датчики (камери), радар.

Радіочастотні аналізатори - це пасивні радіопристрою, які складаються з однієї або декількох антен для прийому радіохвиль та процесора для аналізу радіочастотного спектру. Вони використовуються на коротких відстанях для виявлення каналу радіозв'язку між дроном та його станцією, що управляє. При цьому деякі з них можуть визначати найпоширеніші моделі дронів або MAC-адреси як дрону, так і станції управління, особливо це стосується роботи в діапазоні Wi-Fi. Інші системи також можуть тріангулювати положення дрона та його станції керування при використанні декількох радіомодулів, розміщених у віддаленні один від одного.

Система з акустичних сенсорів (мікрофонів) є групою/набором мікрофонів, які вловлюють звук, що видається дроном, і визначають за допомогою тріангуляції напрямок на нього. Така пасивна система виявляє всі дрони в ближній зоні, у тому числі працюючі автономно. Виявляє дрони в умовах перешкод від землі. Однак дальність роботи акустичної системи обмежена невеликою відстанню до 500 м і дуже погано працює у шумній обстановці.

Оптичні сенсори (камери, матриці) можуть бути стандартними відеокамерами денного світла, так і інфрачервоними або тепловізійними. Вони надає зображення дрона та його корисного навантаження. Оптичні датчики мають високий рівень помилкових спрацьовувань, і погана робота у темряві, тумані та інших атмосферних турбулентності.

Радар – пристрій використовує радіохвилі для виявлення об'єкта. Радар випромінює сигнал і отримує відбитий сигнал від дрона, вимірює напрямок і відстань (положення) до об'єкта. Більшість радарів посилають свій радіосигнал у вигляді пакета, а потім прослуховують «луна». Багато радарів спроектовані так, щоб не виявляти дрібні цілі. Вони призначені для відстеження великих об'єктів, як-от літаки.

Системи для протидії дронам. У випадку заходи протидії дронам можна розділити на: фізичне знищення, нейтралізація, управління (захоплення). До обладнання протидії дронам відносяться: Radio Frequency Jammers, GPS Spoofer, High Power Microwave (HPM) devices, Nets and Guns, High-energy lasers, Birds of Prey.

Подавлювачі радіочастот або радіочастотний глушник (Radio Frequency Jammers) - це стаціонарний або портативний пристрій, який передає через

радіоканал великий потік енергії у бік дрону, маскуючи сигнал оператора. Така дія може призвести до того, що дрон здійснює керовану посадку в поточному положенні, повертається в задане користувачем домашнє місце, безконтрольно падає на землю або летить у випадковому напрямку. Такі пристрої можуть призвести до непередбачуваної поведінки дрона та створити радіоперешкоди іншим радіозасобам.

GPS-ошуканці посилають свій новий сигнал дрону, підміняючи зв'язок із супутниками GPS, які використовуються для навігації. Таким чином, дрон «обманюється» та отримує дезорієнтацію. Динамічно змінюючи GPS-координати в режимі реального часу, такий пристрій може контролювати положення дрону. Як тільки управління буде отримано, дрон може бути спрямований, наприклад, у «потрібному напрямку». Однак застосування таких пристроїв обмежено малою дальністю та можливістю впливу на (глушіння) інших засобів радіозв'язку.

Мікрохвильові пристрої високої потужності генерують великий електромагнітний імпульс (EMI), здатний вивести з експлуатації електронні пристрої. EMI створює перешкоди в радіоканалах та ушкоджує електронні схеми дронів (а також будь-які інші електронні пристрої в межах досяжності). Дані пристрої можуть ефективно не кінетично зупинити дрон, але вони створюють ризик ненавмисного порушення зв'язку або знищення інших електронних пристроїв у зоні дії, а дрон при їх дії миттєво безконтрольно падає на землю.

Сітки та зброя. Стрілянина сітками по дрону або інше контактування сітки з дроном викликає його зупинку та падіння. Така стрілянина мережею може бути реалізована із Землі з дальністю до 300 м, з іншого дрона або за допомогою підвісної мережі, яка розгортається зі спеціального «мережевого» дрону.

Високоенергетичні лазери є потужним енергетично оптичним приладом, що виробляє дуже сильно сфокусований пучок світла в лазерний промінь. Лазер вражає дрон, руйнуючи структуру та/або електроніку, проте має високу вартість, ризик побічної шкоди та великі габарити.

Література

1. Advanced in the telecommunications 2019: monograph / by edited M.Y. Ilchenko, S.O. Kravchuk, Kyiv, 2019, 336 p. (ISBN 978-617-7734-12-2).
2. Kaidenko, M., Kravchuk, S. (2023). Principles of Constructing Communication and Control Systems Protected from the Effects of Jamming Attacks for Small-Sized Unmanned Aerial Vehicles. In: Ilchenko, M., Uryvsky, L., Globa, L. (eds) Progress in Advanced Information and Communication Technology and Systems. MCiT 2021. Lecture Notes in Networks and Systems, vol 548. Springer, Cham. (ISSN2367-3370, E-ISSN2367-3389) – pp. 399-418, https://doi.org/10.1007/978-3-031-16368-5_20
3. Kaidenko M., Kravchuk S. Protection against the effect of different classes of attacks on UAV control channels // Information and Telecommunication Sciences. – No. 1 (2022) . – p. 35-43, DOI: https://doi.org/10.20535/2411-2976.12022.35-43

УДК 621.396.1

РЕЗУЛЬТАТИ АНАЛІЗУ ТЕРМІНОЛОГІЇ В ГАЛУЗІ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ ІЗ ЗАСТОСУВАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Кравчук С.О., Чуб М.М.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail:sakravchuk@ukr.net

THE RESULTS OF THE ANALYSIS OF TERMINOLOGY IN THE FIELD OF ELECTRONIC COMMUNICATIONS USING ARTIFICIAL INTELLIGENCE

With the release of the new law of Ukraine "On Electronic Communications", with the significant spread of new terms in the field of information technology (IT) and Telecom, it becomes quite urgent to analyze such terminology for its better understanding with the help of a powerful AI toolkit.

На даний час значний інтерес прикуто до практичної апробації діалогових систем штучного інтелекту (ШІ). З виходом нового закону України «Про електронні комунікації», зі значним поширення нових термінів в галузі інформаційних технологій (ІТ) та Телекому, стає досить актуальним проведення аналізу такої термінології для її кращого розуміння за допомогою потужного інструментарію ШІ [1-4]. В якості такого інструменту було обрано чат-бот ChatGPT (https://chat.openai.com/), що призначений для ведення діалогів на базі нейромережі, розробленої лабораторією ШІ корпорації OpenAI LP. Загалом, ChatGPT може допомогти дослідникам з виконання певних задач. Однак, таким сервісом не слід зловживати. Можна виділити ряд корисних функцій ChatGPT: переклад тексту, розпізнавання мови, створення програмних кодів, підбір та аналіз інформації, пошук нових ідей досліджень, оформлення додатків та ілюстрацій. Головне, що нам потрібно, це можливість такого чат-боту проводити аналіз величезної кількості світових інформаційних джерел.

Почнемо наш діалоговий аналіз (запитань та відповідей) із найбільш вживаних термінів: телекомунікації, електронні комунікації та інфокомунікації.

Перше завдання аналізу – *який з перерахованих вище термінів є найбільш вживаним?* На сьогодні найбільш вживаним виявився термін "інфокомунікації", оскільки він (на думку ШІ) ширше охоплює всі аспекти обміну інформацією, включаючи телекомунікації та електронні комунікації, а також інформаційні технології та інформаційні системи. Термін "телекомунікації" зазвичай відноситься до передачі голосу, даних та відео за допомогою телефонії, телевізійних мереж та інших *засобів комунікації*. Термін "електронні комунікації" зазвичай відноситься до передачі даних та електронних повідомлень через мережі Інтернет. Однак, у залежності від контексту та галузі, *може використовуватися будь-який з цих термінів*.

Чи не є термін телекомунікації застарілим? Термін "телекомунікації" не є застарілим, оскільки він продовжує використовуватися в різних галузях, пов'язаних з передачею даних, голосу та відео, а також в технічних специфікаціях, стандартах та законодавчих документах з регулювання

засобів масової інформації та зв'язку. Однак, з розвитком технологій та збільшенням обсягів обміну інформацією, у широкому вжитку стали використовувати терміни "електронні комунікації" та "інфокомунікації", які охоплюють більш широкий спектр засобів та технологій обміну інформацією. Таким чином, термін "телекомунікації" може використовуватися у випадках, коли мова йде про конкретні види комунікації через певні канали зв'язку.

Так що краще використовувати телекомунікації або електронні комунікації? Вибір між термінами "телекомунікації" та "електронні комунікації" залежить від контексту та мети використання. Якщо мова йде про передачу голосу, даних та відео через телефонію, телевізійні мережі та інші засоби комунікації, то можна використовувати термін "телекомунікації". Якщо ж мова йде про передачу електронних повідомлень через мережі Інтернет, то краще використовувати термін "електронні комунікації". Проте, у загальному контексті, коли мова йде про обмін інформацією будь-якого типу, можна використовувати більш широкий та універсальний термін "інфокомунікації", який охоплює широкий спектр засобів та технологій, що використовуються для обміну інформацією та комунікації, таких як мережі зв'язку, Інтернет, соціальні мережі, електронна пошта, мобільні додатки, онлайн-громадськість та інші. Цей термін відображає зміну в технологічних та соціальних тенденціях, де обмін інформацією стає все більш важливим і все більше пов'язаним з технологічними засобами.

Чим відрізняються інфокомунікаційні та інформаційно-комунікаційні системи? Інформаційно-комунікаційні системи (ІКС) та інфокомунікації пов'язані між собою, але вони *не є тотожними*. ІКС - це комплексна система обробки, передачі, збереження та відтворення інформації з використанням різних технологій комунікацій та інформаційних технологій. ІКС забезпечують інфраструктуру для різноманітних інформаційних послуг, таких як електронна пошта, відеозв'язок, доступ до Інтернету, передача даних та інші. Інфокомунікації - це процес обміну інформацією з використанням будь-яких доступних технологій. Інфокомунікації можуть включати в себе такі засоби, як мережі зв'язку, комп'ютери, мобільні пристрої, соціальні мережі, електронна пошта, телебачення, радіо та інші засоби комунікації.

Іншими словами, ІКС забезпечують технічну базу для інфокомунікацій, тоді як інфокомунікації охоплюють ширший спектр взаємодії людей та організацій з використанням будь-яких доступних технологій для обміну інформацією.

Що представляють собою послуга, технологія і система електронних комунікацій? Послуга електронних комунікацій охоплює будь-які послуги передачі, обробки та отримання інформації, що використовують електронну технологію.

Технології електронних комунікацій включають у себе всі електронні пристрої, мережі, програмне забезпечення та протоколи, які використовуються для передачі даних, голосу, відео та іншої інформації. Ці технології можуть бути бездротовими або провідними, залежно від того, як передається інформація.

Система електронних комунікацій - це комплекс технічних засобів та програмного забезпечення, які забезпечують передачу, обробку, збереження та отримання інформації. Вона може складатися з різноманітних

компонентів, таких як мережі передачі даних, телефонні системи, мережі Інтернет тощо.

Соціальні мережі охоплені термінами телекомунікації та електронні комунікації? Соціальні мережі можна вважати одним з видів електронних комунікацій, оскільки вони дозволяють користувачам обмінюватися повідомленнями та іншою інформацією через Інтернет. Проте, термін "електронні комунікації" не відображає повністю всіх аспектів соціальних мереж як феномену, оскільки соціальні мережі також включають в себе можливості для створення спільнот, обміну думками, дослідження даних та інші функції, які не пов'язані безпосередньо з комунікацією.

Електронні комунікації та телекомунікації є частинами інфокомунікацій? Так, електронні комунікації та телекомунікації є частинами інфокомунікацій. Інфокомунікації - це широкий термін, який охоплює будь-який обмін інформацією, що відбувається з використанням різних технологій, включаючи електронні комунікації та телекомунікації. Електронні комунікації використовуються для обміну інформацією за допомогою електронних засобів, таких як електронна пошта, миттєві повідомлення, відеозв'язок тощо. Телекомунікації охоплюють передачу інформації за допомогою мережі зв'язку, такої як телефонні мережі, мережі передачі даних, супутникові мережі та інші. Таким чином, електронні комунікації та телекомунікації є двома головними складовими інфокомунікацій.

Як повязані терміни електрозвязок і телекомунікації? Терміни "електрозв'язок" і "телекомунікації" мають певну спільність, оскільки обидва описують передачу інформації на відстань за допомогою електричних сигналів. Однак, термін "електрозв'язок" є більш старим і зазвичай використовується для опису традиційних методів передачі голосової інформації на відстань, таких як телефонія з використанням проводів, радіовипромінення, а також телеграфування. Термін "телекомунікації" є більш широким та універсальним, і він включає в себе термін "електрозв'язок" як один з його аспектів.

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. Кравчук С.О. Теорія систем мобільних інфокомунікацій. Системна архітектура [Електронний ресурс]: навчальний посібник за спеціальністю 172 «Телекомунікації та радіотехніка» / С. О. Кравчук; КПІ ім. Ігоря Сікорського. – Електронні текстові данні (1 файл: 18,17 Мбайт). – Київ: КПІ ім. Ігоря Сікорського, 2023. – 683 с. - https://ela.kpi.ua/handle/123456789/53198.
4. Прикладні аспекти системного аналізу в телекомунікаціях та радіотехніці: Методичні рекомендації до виконання практичних занять [Електронний ресурс] : навч. посіб. для студ. спеціальності 172 «Телекомунікації та радіотехніка» / КПІ ім. Ігоря Сікорського; уклад.: С.О. Кравчук, О. І. Лисенко, В. С. Явіся, В. І. Новіков. – Електронні текстові дані (1 файл: 1,48 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 46 с. Кількість авторських аркушів: 2.3. Дата затвердження: 2021-06-24. Номер протоколу: 8. Примірник надано до бібліотеки у електронній формі: https://ela.kpi.ua/handle/123456789/41977.

УДК 520.6.05

СПОСІБ ПІДВИЩЕННЯ КОЕФІЦІЄНТА ПОСИЛЕННЯ ПРИЙМАЛЬНО-ПЕРЕДАВАЛЬНОГО ОБЛАДНАННЯ КАНАЛУ ЗВ'ЯЗКУ З ДРОНАМИ

Явіся В.С., Лисенко О.І., Гетьман О.В.
Навчально науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: yavisya42@gmail.com

THE METHOD OF INCREASING THE AMPLIFICATION COEFFICIENT OF THE RECEIVING AND TRANSMITTING EQUIPMENT OF THE COMMUNICATION CHANNEL WITH DRONES

When using drones, it is necessary to ensure the transmission of a large amount of data with a given bandwidth and bit error probability. For this, it is necessary to provide measures that allow to ensure the required energy level of the transmitted signal. Such a task can be solved by using directional antennas both on the ground control complex and on board the drone.

За допомогою мультикоптерних дронів можна контролювати технічний стан об'єктів, їх безпеку та режими функціонування, здійснювати аерофотознімання для картографування, дрони можуть доставляти вантажі, бути основою телекомунікаційної повітряної платформи і т.п. [1].

При застосуванні дронів необхідно забезпечити передачу великого обсягу даних при заданих смузі пропускання й імовірності бітової помилки.

Для задоволення вимог по пропускній здатності доцільним є вибір надвисоких частот (НВЧ), а саме, діапазону 2,4 ГГц [2].

Зазвичай дрони використовуються на відстанях до 10 км. У діапазоні 2,4 ГГц загасання сигналу на відстані 10 км досягає 120 дб [2], тому необхідно передбачити заходи, що дозволяють забезпечити необхідний енергетичний рівень переданого сигналу на такий відстані. Аналіз ринку малогабаритних приймально-передаючих пристроїв показує, що найпоширеніші приймачі із чутливістю порядку –90 дб, і передавачі з посиленням близько 30 дб, що дозволяє перекрити загасання в 120 дб.

Наприклад, для забезпечення ймовірності помилки порядку 10^{-6} при використанні QAM32 на вході приймача необхідно забезпечити відношення сигнал/шум на рівні 18 дб [2]. Враховуючи втрати у фідері приймача й передавача (усього близько 3 дб), стає зрозумілим, що енергетика переданого сигналу повинна бути збільшена, як мінімум, на 21 дб, а в реальних умовах поширення сигналу й впливу ненавмисних перешкод – на ще більшу величину. Розв'язати таке завдання можна шляхом використання спрямованих антен як на наземному комплексі управління (НКУ), так і на борті дрона.

На НКУ можна використати параболічну антену, коефіцієнт підсилення якої для прийнятних ваго-габаритних показників (при діаметрі дзеркала до 0,5 м) складе не більше 19 дб. Подальше підвищення коефіцієнта підсилення може бути здійснене за рахунок збільшення діаметра дзеркала, що важко реалізувати для носимих НКУ. Зрозуміло, що рівень сигналу повинен бути

підвищений «із запасом» приблизно на 5 дб.

Управління напрямком максимального посилення бортової антени може здійснюватися декількома способами [2]: установка антени на опорно-поворотному пристрої; використання багатоелементної антенної решітки з керованою діаграмою спрямованості; використання декількох антен, що перемикаються.

Реалізація першого способу дозволяє використовувати одну гостроспрямовану антену для безперервного спостереження за напрямком на НКУ. При установці антени на опорно-поворотному пристрої необхідне створення обертового переходу. Він може бути розміщений у різних місцях: перед антеною після підсилювача потужності; після передавача перед підсилювачем потужності й антеною; передавальний пристрій, підсилювач потужності й антена розміщуються на поворотному пристрої, через багатоканальний обертовий перехід передаються сигнали та живлення.

Загальними недоліками використання опорно-поворотного пристрою є:

- висока вартість обертового коаксіального НВЧ переходу;
- при розміщенні гостроспрямованої антени будь-якого типу на опорно-поворотному пристрої, більша частина поверхні поворотної платформи залишається невикористаною.;
- переміщення антени в горизонтальній площині приводить до переміщення центру ваги дрону, а отже до дестабілізації його просторового положення;
- значні витрати потужності на роботу електропривода.

При реалізації другого способу для створення антенної системи з керованою діаграмою спрямованості може бути використана кільцева антенна решітка. Завдяки кільцевій симетрії антенної решітки вдається одержати спрямовані діаграми, які мало змінюються при скануванні в межах 360º у площині решітки.

Однак, для одержання посилення кільцевою антенною решіткою необхідно збільшувати число елементів, що у зв'язку з ваго-габаритними обмеженнями неприйнятно для мультикоптерних дронів з електроприводом. Крім того, використання багатоелементної антенної решітки ускладняється необхідністю виготовлення складних і високовартісних діаграм утворюючих пристроїв.

Третій спосіб передбачає використання декількох антен, що перемикаються, тоді просторові напрямки по азимуту розбиваються на сектори. Зі збільшенням коефіцієнтів підсилення антен їх число зростає, а для розміщення великої кількості антен потрібно збільшувати габаритні розміри й масу всієї антенної системи. У цьому випадку можливий компромісний розв'язок, що забезпечує необхідне посилення й задовольняє ваго-габаритні обмеження.

Для його реалізації пропонується розмістити на борту дрона шість антен типу «хвильовий канал». З урахуванням ваго-габаритних обмежень конструкція однієї антени буде складатися лише із трьох елементів.

Розміри елементів антени визначаються довжиною хвилі, а саме: активний вібратор $A = 0{,}5\lambda$; рефлектор незначно більше вібратора $R \geq A$; директор незначно менше його $D \leq A$; відстань між рефлектором, активним вібратором і директором $l = 0.25\lambda$. Для обраного частотного діапазону

$\lambda = 0{,}125$ м, тому одна антена має габарити приблизно 7х7 см, а конструкція із шести антен вписується в окружність радіусом $R_6 = 2l + l\sin 60 \approx 9$ см, а її вага складе близько 120 грам. Коефіцієнт підсилення трьохелементної антени типу «хвильовий канал» – 5,5 дб [2].

При наявності декількох антен на борту дрона виникає необхідність вибору антени, спрямованої убік НКУ. Існує кілька варіантів реалізації подібної системи: перемикання виходу підсилювача передавача між антенами (один передавач, один підсилювач потужності, кілька антен); перемикання виходу передавача між підсилювачами потужності й антенами (один передавач, кілька сполучених підсилювачів потужності й антен); перемикання сигналу між передавачами (число передавачів і підсилювачів потужності дорівнює числу антен).

При першому варіанті вихідний сигнал підсилювача потужності комутирується між декількома антенами. Гідністю цього варіанта є використання єдиного передавального модуля й підсилювача потужності для роботи на кілька антенних пристроїв. Загальним недоліком є втрати в комутуючому пристрої.

При другому варіанті число підсилювачів потужності дорівнює числу антен. До недоліків такого підходу можна віднести: наявність декількох підсилювачів потужності, які займають багато місця й мають більшу вагу.

Третій варіант вимагає використання для кожної антени свого передавача й підсилювача потужності. У цьому випадку перемикач сигналів виконується на рівні цифрової логіки. До переваг даного підходу слід віднести високу надійність системи. Однак платою за це є велика вага й висока вартість.

Очевидно, що для дронів кращим є перший варіант – тобто перемикання виходу підсилювача потужності передавача між антенами.

Таким чином, при використанні запропонованого варіанта побудови антенної системи загальне посилення приймально передавального обладнання каналу зв’язку з дронами може бути значно збільшене, що забезпечить можливість здійснення високошвидкісної та якісної передачі інформації на значні відстані з низькою імовірністю помилки.

Література

1. Lysenko, O., Romaniuk, V., Romaniuk, A., Novikov, V., Yavisya, V., Sushyn, I. (2023). The Method of Using a Telecommunication Air Platform as a Flying Info-Communication Robots. In: Ilchenko, M., Uryvsky, L., Globa, L. (eds) Progress in Advanced Information and Communication Technology and Systems. MCiT 2021. Lecture Notes in Networks and Systems, vol 548. pp 357–376. Springer, Cham. https://doi.org/10.1007/978-3-031-16368-5_18. ISSN 2367-3370.
2. Явіся В.С., Лисенко О.І. Спосіб підвищення якості каналу управління дронами // Чотирнадцята міжнародна науково-технічна конференція «Перспективи телекомунікацій». Матеріали конференції. – К.: КПІ ім. Ігоря Сікорського. – 2020. – С. 281-284. ISSN (print) 2663-502X, ISSN (online) 2664-3057.

УДК 621.396

СИСТЕМА ІНТЕРНЕТУ РЕЧЕЙ НА БАЗІ МЕРЕЖІ 5G

Міночкін Д.А., Мацюк Е.О.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: dmytro.minochkin@gmail.com, elinka0112@gmail.com

SYSTEM OF INTERNET OF THINGS BASED ON 5G NETWORK

Due to increasing customer demands, the current architecture of IoT will not be reliable and responsive enough to accommodate next-generation IoT applications and future services. This document proposes the next-generation architecture of IoT based on new technologies that take into account the requirements of future programs, services, and generated data. Specifically, this architecture benefits from new technologies such as Device-to-Device (D2D) communication, 5G-IoT, Machine-Type Communication (MTC), Wireless Network Function Virtualization (WNFV), Wireless Software-Defined Networks (WSDN), Mobile Edge Computing (MEC), and Mobile Cloud Computing (MCC). This combination of technologies is capable of meeting the requirements of new applications. The proposed new architecture is modular, efficient, flexible, scalable, simple, and capable of handling large amounts of data and application requirements.

In this official document, we explore the path to digital transformation with 5G support. This journey will take several years as 5G networks and capabilities gradually become available while previous generations of networks are phased out.

Кевін Ештон припустив, що згодом у кожної з речей реального фізичного світу в IoT буде цифровий двійник, її віртуальне представлення [1].

Глобальний обсяг даних постійно збільшується, що робить розвиненим 5G необхідним і неминучим фактом. Внаслідок такого величезного зростання обсягів даних у середньостроковій перспективі існуючі технології більше не відповідатимуть вимогам світу IoT.

5G IoT виходить на новий рівень у всіх аспектах. Пропускна здатність у новій мережі має досягати 20 гігабіт на секунду, що дозволить скоротити час відгуку. З 5G можна буде також передавати дані в режимі реального часу. Це означає, що 100 мільярдів мобільних пристроїв у всьому світі будуть доступні одночасно. Іншими словами, густина підключення приблизно один мільйон пристроїв на квадратний кілометр. У той же час нова технологія дасть покращення зв'язку під час руху, це означає, що якість зв'язку буде набагато стабільнішою до швидкості 500 кілометрів на годину, що принесе величезні переваги, особливо для користувачів мережі, що подорожують.

Запропоновано архітектуру 5G–IoT .Архітектура складається з восьми пов'язаних між собою шарів з можливістю двостороннього обміну даними, як показано на рис. 1. Другий шар і п'ятий шар складаються з двох і трьох підшарів, відповідно, і рівень безпеки покриває всі інші рівні. Ці шари вибрано для забезпечення найкращої продуктивності та одночасно підтримувати модульність архітектури.

1. Рівень фізичного пристрою.

Цей рівень складається з бездротових датчиків, приводів і контролерів, які насправді є «речами» IoT. Фізичні пристрої є загальним рівнем у всіх архітектурах. У цьому шарі мають бути використані пристрої невеликого розміру, такі як наночіпи щоб збільшити обчислювальну потужність і зменшити потужність споживання. Наночіпи здатні виробляти велику кількість початково оброблених даних, які підходять для Big Data в аналітичному рівні (рівень 5).

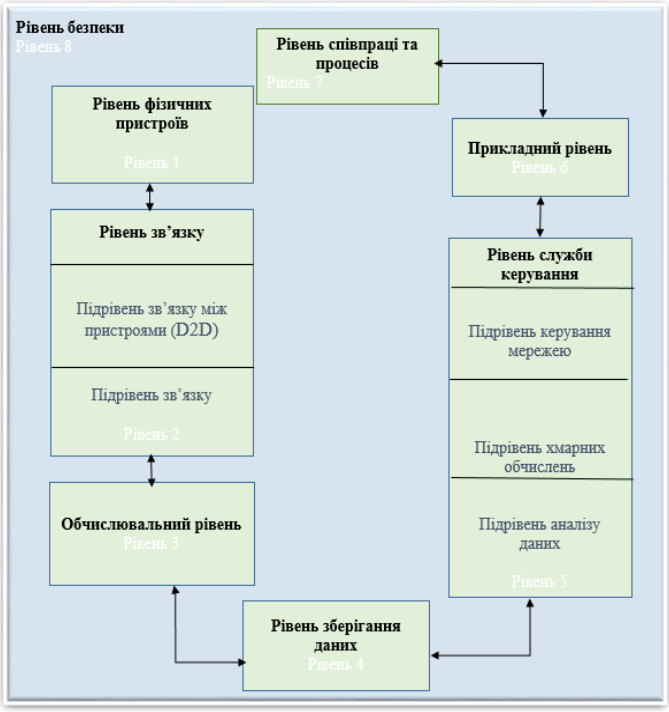


Рис.1. Архітектура 5G–IoT.

2. Рівень зв'язку

Цей шар складається з двох підшарів. Зв'язок D2D і рівні підключення.

• Підрівень прямого зв'язку між пристроями (D2D). Завдяки збільшенню обчислювальної потужності та інтелекту фізичних пристроїв (вузлів) вони містять свої власну ідентичність та особистість і можуть створювати власні дані. Для підвищення ефективності і можливості IoT системи, ці пристрої повинні формувати Неоднорідну мережу (HetNet) для спілкування один з одним. На цьому підрівні використовуються сучасні протоколи зв'язку бездротової сенсорної мережі (WSN).

Вузли можуть створювати кластери або навіть вибирати лідера (голову кластера) для відповідної мережі. Однією з найважливіших технологій, які покращують цей підрівень, це mmWave (міліметрові хвилі). Крім того, на цьому підрівні 5G є ще одна додаткова технологія, яка здатна покращити D2D спілкування. 5G розглядається як важливий кандидат для забезпечення підключення до МТС пристроїв. Завдяки підтримці високої швидкості передачі даних та інші важливих функцій МТС 5G-Plus-HetNet

розглядається як сильне технологічне рішення в запропонованій

архітектурі 5G-IoT, яка забезпечує низьку затримку для IoT.

• Підрівень зв'язку. На цьому підрівні пристрої підключаються до центрів зв'язку, таких як базові станції. Крім того, вони надсилають і аналізують свої дані через центри через підключення до внутрішньої мережі до блоку зберігання. На даний момент цей підрівень IoT має певні проблеми: можна обробляти лише обмежену кількість підключень пристроїв; у програмах, таких як автономні транспортні засоби, обмін даними для різних типів даних не застосовується; великий обсяг даних навряд чи можна обробити в режимі реального часу через велику затримку зв'язку. Найближчим часом розгортання 5G робить значну еволюцію на цьому підрівні в сенсі надійності, продуктивності та гнучкості.

Іншою технологією цього підрівня є Advanced SSIM. Завдяки цій технології пристрої IoT отримують можливість вибору відповідного спектру (діапазонів частот) із

достатньо низькими перешкодами. Насправді методи SSIM є корисними для використання можливостей спільного використання спектру на основі когнітивного радіо. Цей підрівень, розроблений в архітектурі, забезпечує низьку затримку, надійність з'єднань і підтримку різних типів даних.

3. Обчислювальний рівень Edge (Fog).

На цьому рівні дані обробляються вузлами або їх лідерами для прийняття рішень на рівні Edge. З появою технології 5G і розвитком мобільних пристроїв (таких як смартфони) технологія MEC стане більш потужною для подолання викликів і зробить значний внесок на цьому рівні.

4. Рівень зберігання даних

Цей рівень містить блоки зберігання даних, у яких зберігається інформація, отримана від обробки периферії фізичних пристроїв, а також необроблені дані. Цей рівень потребує особливого захисту з точки зору безпеки, а також повинен реагувати на величезний обсяг даних і трафік майбутніх програм.

5. Рівень служби керування.

Цей рівень складається з трьох підрівнів.

• Підрівень керування мережею. Управління мережею передбачає зміну типу зв'язку між пристроями та центрами обробки даних. Найважливішою технологією, задіяною в цьому підрівні, є WNFV. WNFV може одночасно оновлювати топологію мережі та тип протоколів зв'язку, наприклад 5G-IoT або ZigBee, для покращення якості структури IoT. Іншою корисною технологією на цьому підрівні є WSDN. WSDN керує мережею IoT і дозволяє змінювати конфігурацію мережі замість традиційного моніторингу мережі для підвищення продуктивності.

• Підрівень хмарних обчислень. На цьому підрівні дані та інформація з периферійних обчислень (повторно) обробляються в хмарі, щоб можна було отримати остаточну оброблену інформацію. Завдяки впровадженню технології 5G мобільні пристрої можуть виконувати цей тип обчислень, який називається MCC, у режимі реального часу. Таким чином, операції обробки будуть розподілені між мобільними пристроями паралельно, щоб зробити систему IoT більш ефективною, стійкою, масштабованою та швидшою.

• Підрівень аналізу даних. На цьому підрівні використовуються нові методи аналізу даних [9] для створення цінності (інформації, яку можна маніпулювати) із вихідних даних. Будь-яке вдосконалення алгоритмів великих даних покращить обробку даних на цьому підрівні. Насправді роль цього домінуюча у найближчому майбутньому, коли кількість зібраної інформації збільшиться завдяки інтеграції 5G та IoT.

6. Прикладний рівень

На цьому рівні програмне забезпечення взаємодіє з попередніми рівнями та даними, які перебувають у стані спокою, тому немає необхідності працювати на швидкості мережі. Додатки здатні революціонізувати вертикальні ринки та бізнес-потреби, керуючи програмами, вертикальними та мобільними додатками, бізнес-аналітикою та аналітикою. Фактично, прикладний рівень дозволяє бізнесменам робити правильні речі в потрібний час з потрібними даними.

7. Рівень співпраці та процесів

Система IoT та інформація, що надходить із попередніх рівнів, не корисні, якщо

вони не створюють акт. Люди використовують програми та пов'язані з ними дані для власних потреб. Іноді кілька осіб використовують одну програму для різних цілей. Насправді люди повинні мати можливість співпрацювати та спілкуватися, щоб зробити IoT придатним для обслуговування.

8. Рівень безпеки

Цей рівень вважається окремим. Насправді цей рівень охоплює та захищає всі попередні шари, але кожен розділ (точка перетину цього шару з іншим) має власну функціональність. Рівень безпеки запропонованої архітектури передбачає різні терміни функцій безпеки, включаючи шифрування даних, автентифікацію користувачів, контроль доступу до мережі та захист хмари [3]. Крім того, рівень безпеки також запобігає та передбачає небезпеки та кібератаки, включаючи криміналістику для виявлення типу атаки та її поразки.

Висновки. Архітектури, засновані на технології зв'язку 5G, здатні задовольнити вищевказані вимоги та забезпечити такі характеристики: простота управління, надійність, можливість реконфігурації, високий рівень безпеки, легке та швидке усунення несправностей, широке покриття, низька вартість розгортання. Архітектура, розроблена в цьому документі, забезпечує низьку затримку завдяки використанню комунікацій 5G і D2D, а також надійність з'єднань завдяки MTC і Het-Net.

Крім того, він підтримує різні типи даних завдяки перевагам 5G. Фактично, завдяки інтеграції 5G та IoT багато інших технологій, таких як MTC і WNFV, можуть взяти участь в архітектурах IoT наступного покоління. Відповідна комбінація цих технологій може створити більш комплексну структуру, яка відповідає переліченим вимогам додатків IoT наступного покоління.

Література

1. Навчальний посібник «Технології Інтернету речей» [Електронний ресурс] – Б.Ю. Жураковський, І.О. Зенів – Режим доступу до ресурсу: https://ela.kpi.ua/bitstream/123456789/42078/1/Zhurakovskyi_B_Zeniv_Tehnologii_internet_rechey.pdf
2. Comprehensive Survey of Key Technologies Enabling 5G-IoT [Electronic resource] –Mode of access: https://www.researchgate.net/publication/332407851_Comprehensive_Survey_of_Key_Technologies_Enabling_5G-IoT
3. M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities." Elsevier, 2018.
4. 5G and IoT: What can 5G do for IoT business? [Electronic resource] – Mode of access: https://iot.telenor.com/iot-insights/5g-and-iot/
5. 10 Ways Machine Learning Is Revolutionizing Manufacturing http://www.forbes.com/sites/louiscolumbus/2016/06/26/10-waysmachine-learning-is-revolutionizing-manufacturing/#57d0ec792d7f Retrieved: Oct, 2016
6. 5G IoT: What does 5G mean for IoT? [Electronic resource] – Mode of access: https://www.avsystem.com/blog/5g-iot/

УДК 621.39

ОЦІНКА НАУКОВОГО НАПРЯМУ ДОСЛІДЖЕНЬ ГОЛОСОВИХ ПОСЛУГ У МЕРЕЖАХ 5-ГО ПОКОЛІННЯ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ CHATGPT

Ветошко І.П.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: ivan.vetoshko@ukr.net

EVALUATION OF THE SCIENTIFIC DIRECTION OF VOICE SERVICES RESEARCH IN 5TH GENERATION NETWORKS BASED ON ARTIFICIAL INTELLIGENCE CHATGPT

In the course of the work, an assessment of the scientific direction of research on voice services in 5th generation networks based on artificial intelligence ChatGPT was considered. The results of an empirical study of ChatGPT and its potential contribution to science are presented.

В ході роботи було розглянуто оцінку наукового напряму досліджень голосових послуг у мережах 5-го покоління на основі штучного інтелекту ChatGPT. Приведено результати емпіричного досліду роботи ChatGPT та його потенційний внесок у науку.

У сучасному світі розвиток нових технологій займає фундаментальне місце. Однією з провідних інженерних технологій є штучний інтелект (Artificial Intelligence, AI). У загальному розумінні, AI – це комп’ютерна система, яка здатна виконувати завдання, для виконання яких зазвичай потрібен людський інтелект. Залучення таких інструментів, як штучний інтелект, до наукових досліджень, може пришвидшити та полегшити отримання результатів. У свою чергу AI вміє оперувати великим обсягом даних за лічені секунди. Це може надати багато переваг порівняно з дослідженнями де штучний інтелект не використовується.

Наразі існують різні типи та ресурси штучного інтелекту. Популярними AI ресурсами є: TensorFlow, OpenAI, Keras, PyTorch, Character AI, Machine Learning Mastery та інші. Проте, найбільш прогресивним є мовна модель ChatGPT від однієї з провідних світових дослідницьких організацій штучного інтелекту Open AI. Як мовна модель, ChatGPT призначений для обробки та генерування людської мови, використовуючи передові методи машинного навчання для навчання на великих обсягах текстових даних. В основі ChatGPT лежить трансформаторна архітектура, яка є типом нейронної мережі, що чудово справляється з обробкою послідовних даних, таких як текст [1].

Варто розглянути й оцінити вплив та внесок даного продукту на прикладі дослідження голосових послуг у мережах 5-го покоління. Оскільки згадана наукова проблематика є безсумнівно актуальною, то даний аналіз може показати реальний результат роботи штучного інтелекту ChatGPT. З практичної точки зору, використання AI, під час пошуку рішення щодо

реалізації голосових послуг у мережах 5G, може запропонувати нові ідеї, ну або ж ті, що на перший погляд могли б не спати. Важливою умовою досліджень є критерії якості надання голосових послуг у мережах 5G мобільного зв’язку та вимоги до KPI-параметрів передачі голосового трафіку.

Спробуємо запитати у ChatGPT, як він оцінює науковий напрям досліджень голосових послуг у мережах 5-го покоління (рис. 1).

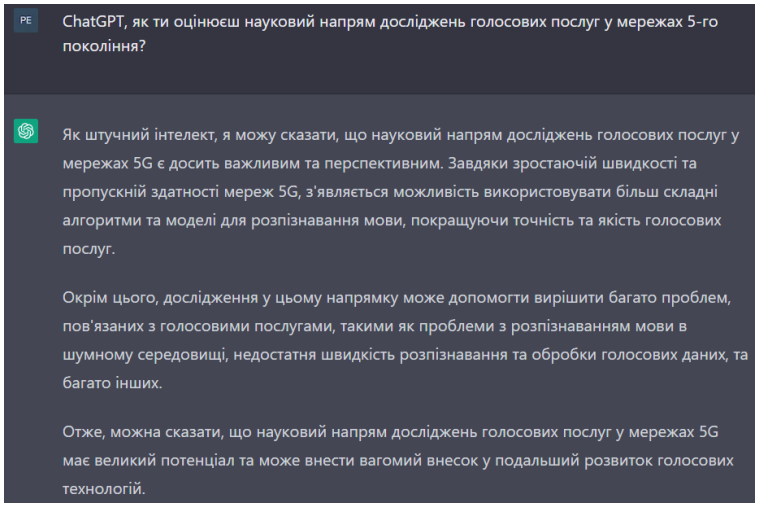


Рис. 1. Оцінка штучним інтелектом ChatGPT наукового напряму досліджень голосових послуг у мережах 5-го покоління.

Як видно з відповіді, шо надав ChatGPT , він дійсно розуміє важливість досліджень даної теми, розуміє про перспективи та оцінює потенціал вирішення певних проблем у ході досліджень [3]. Хоч відповідь була надана досить лаконічна, проте хід думок є послідовним та вірним. Також цікаво дізнатись думку штучного інтелекту з приводу важливості дослідження критеріїв якості надання голосових послуг у мережах 5G мобільного зв’язку та вимоги до KPI-параметрів передачі голосового трафіку (рис. 2).

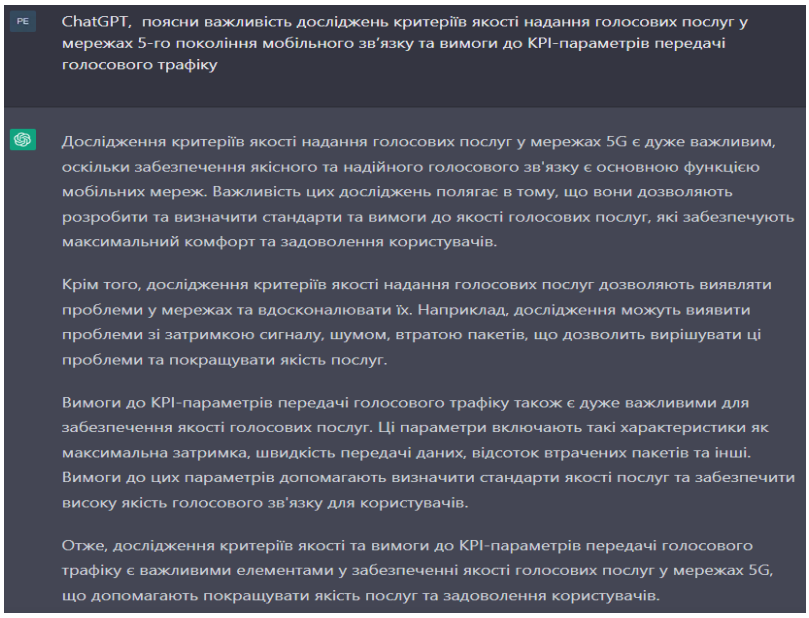


Рис. 2. Оцінка штучним інтелектом ChatGPT важливості дослідження критеріїв якості надання голосових послуг у мережах 5G мобільного зв’язку та вимоги до KPI-параметрів передачі голосового трафіку.

Дана відповідь штучного інтелекту приємно вражає. Як і в попередньому випадку, відповідь є лаконічною та містить власний аналіз із зазначеним висновком сказаного. Тобто, на перший погляд, досить нелегко зрозуміти, що дана відповідь була надана не фахівцем у цій галузі «живою людиною», а штучним інтелектом. Такий результат безсумнівно є частиною наукового прогресу, враховуючи постійну роботу над покращеннями роботи даного штучного інтелекту від Open AI. Іншими словами, він може надати дослідникам широкий діапазон інформації та знань з багатьох різних областей, що може допомогти у вирішенні різних проблем та завдань. Особливо це актуально, для сфери інформаційних технологій та телекомунікацій, які є рушійною силою технологічного прогресу [2].

Переваги використання ChatGPT численні. По-перше, ChatGPT дуже точно генерує зв'язну і контекстуально релевантну мову, що робить його ідеальним інструментом для широкого спектру завдань з обробки природної мови. По-друге, ChatGPT можна точно налаштувати під конкретні завдання, що дозволяє організаціям або ж науковцям адаптувати модель до своїх конкретних потреб.

Однак, у використанні ChatGPT є і деякі потенційні недоліки. Одна з них полягає в тому, що модель може увічнити упередження та стереотипи, які присутні в навчальних даних. Наприклад, якщо модель навчається на наборі даних, що вже втратили актуальність або на межі втрати актуальності. Крім того, оскільки ChatGPT є мовною моделлю, вона не має глибокого розуміння основних концепцій і значень, що лежать в основі мови, яку вона генерує. Це може призвести до непорозумінь або помилок у певних контекстах [3].

Підсумовуючи, можна сказати, що штучний інтелект ChatGPT є досить корисним інструментом при оцінці наукового напряму досліджень голосових послуг у мережах 5-го покоління, оскільки він має величезну базу знань та може надавати відповіді з елементами аналізу. Крім того, ChatGPT може бути корисним для генерації нових ідей та підходів до дослідження. Також, враховуючи надані відповіді штучним інтелектом, він може забезпечити швидкий та легкий доступ до великої кількості інформації, що допоможе зробити дослідження більш ефективним та результативним.

Література

1. Introducing ChatGPT // [Електронний ресурс] режим доступу: https://openai.com/blog/chatgpt
2. ChatGPT helper // [Електронний ресурс] режим доступу: https://chat.openai.com/chat
3. What are the advantages and disadvantages of ChatGPT in digital marketing? // [Електронний ресурс] режим доступу: https://www.quora.com/What-are-the-advantages-and-disadvantages-of-Chat-GPT-in-digital-marketing

УДК 621.396.1

ДОСЛІДЖЕННЯ МЕТОДІВ МОНІТОРИНГУ ТРАФІКУ ДЛЯ ПРОТИДІЇ ФРОДУ В IP-ТЕЛЕФОНІЇ

Карпишин Н.Я., Кравчук С.О.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: nazar.karpishin@gmail.com

RESEARCH OF TRAFFIC MONITORING METHODS TO ANTI-FRAUD IN IP-TELEPHONY

Curr ides many advantages al circuit-switched s

На д ирення, оскільки олів для передачі аналів.

Зрос наведено зростанн у часі за допомог over IP).

Рис. 1. Залежність прогнозу збільшення капіталу VOIP ринку від часу, в роках (Джерело: ZionResearchAnalysis 2016 р.)

Технологія 5G (П’яте покоління мобільних мереж) може відіграти важливу роль у розвитку Voice over Internet Protocol (VoIP), тобто телефонії через Інтернет.

5G має значно більшу пропускну здатність та швидкість передачі даних порівняно з попередніми версіями мобільних мереж, що може забезпечити високоякісну передачу голосу в реальному часі з мінімальним затримкою. Це може бути особливо корисно для VoIP, де якість зв'язку має велике значення.

Завдяки 5G мережі, користувачі VoIP можуть відчувати більш стабільне та якісне з'єднання, яке забезпечує більшу якість передачі голосу та зменшення затримки. Крім того, зв'язок через 5G мережу може бути більш безпечним та захищеним, що дозволяє користувачам відчувати себе більш упевненими у тому, що їхні особисті дані захищені.

Стрімкий ріст цікавості до технологій штучного інтелекту не був проігнорований і в сфері VOIP. Штучний інтелект та машинне навчання вже можуть розпізнавати мову та аналізувати дані дзвінків. І з розвитком цієї галузі очікується автоматична відправка кореспонденції та доставка. Крім

того, штучний інтелект зможе виявляти та реагувати на помилки та несправності.

Також розвиток штучного інтелекту може суттєво допомогти в протидії шахрайству в IP телефонії. Серед варіантів - моніторинг трафіку. Завдяки машинному навчанню, система може навчитись розпізнавати ненормальні патерни в трафіку, що можуть свідчити про спроби шахрайства. Наприклад, якщо виявлено, що дзвінки з одного номера здійснюються до багатьох різних номерів одночасно, це може свідчити про автоматизований шахрайський процес.

ШІ може використовуватись для автоматичного виявлення підозрілих транзакцій та підозрілих дзвінків на основі аналізу поведінки користувачів, історії транзакцій та інших факторів. Таким чином, штучний інтелект може допомогти виявляти шахраїв, які використовують телефонні мережі для здійснення шахрайства та інших злочинних дій. Крім того, штучний інтелект може допомогти вдосконалити систему авторизації та ідентифікації користувачів, забезпечуючи високий рівень безпеки та захисту від несанкціонованого доступу до системи. Він також може допомогти управляти ризиками та покращити ефективність боротьби з фродом у мережі IP телефонії.

В цілому, застосування штучного інтелекту в моніторингу трафіку для протидії фроду в IP телефонії може допомогти забезпечити високий рівень безпеки та ефективності мережі, зменшити ризики від шахраїв та інших злочинців, а також підвищити рівень задоволення користувачів.

Мета роботи полягає в тому, щоб шляхом дослідження доступних методів моніторингу трафіку розробити нові та/або удосконалити наявні, для оптимізації протидії шахрайству в IP телефонії. Це дозволить зменшити фінансові та репутаційні ризики, як для компаній провайдерів, так і для їх клієнтів.

Фрод (англ. fraud) - це шахрайство або обман, який зазвичай виконується з метою отримання незаконної вигоди, часто фінансової. Фрод в IP-телефонії є серйозною проблемою в сучасному світі. IP-телефонія, як технологія передачі голосу через Інтернет, стала дуже популярною в останні роки, із зростанням популярності вона стала більш вразлива на шахрайство.В свою чергу можна виділити деякі з найпоширеніших видів порушень: tollfraud , рефайл, злом провайдерського або клієнтського обладнання. (АТС, IPPBX).

Серед найбільш дієвих методів протидії фроду слід виділити моніторинг трафіку в мережі, який дозволяє ефективно протидіяти порушенням. Також слід виділити саме методи моніторингу трафіку серед яких:

1. Packet Sniffing: цей метод забезпечує збір даних, які передаються через мережу IP телефонії. Цей метод можна виконати за допомогою програмного забезпечення, такого як Wireshark, і дозволяє перевіряти вміст кожного пакету.

2. Deep Packet Inspection (DPI): цей метод забезпечує збір додаткових даних з кожного пакету, таких як IP-адреси та номери телефонів. DPI дозволяє здійснювати детальний аналіз трафіку, виявляти шкідливі програми та виявляти аномальну активність.

3. NetFlow Analysis: цей метод дозволяє збирати дані про трафік та аналізувати його. Інформація про трафік, що передається через IP телефонію, записується в форматі NetFlow та може бути аналізована, щоб виявити аномальну активність.

4. Call Detail Record (CDR) Analysis: цей метод забезпечує збір даних про кожен телефонний дзвінок, включаючи час дзвінка, тривалість та номери, що беруть участь. Ці дані можуть бути аналізовані для виявлення незвичайної активності та шахрайства.

5. Real-time Monitoring: цей метод забезпечує моніторинг мережі IP телефонії в режимі реального часу. Це дозволяє виявляти проблеми в мережі та шкідливі дії в момент їх виникнення.

Комбінування різних методів моніторингу трафіку, таких як аналіз поведінки користувачів, виявлення аномального трафіку та використання сигнатур для ідентифікації фроду, дозволяє створити більш комплексну систему захисту від шахрайства в ip-телефонії.

Така комбінація методів моніторингу трафіку дозволяє збільшити точність виявлення фроду та знизити кількість помилкових спрацювань системи захисту. Наприклад, виявлення аномального трафіку може доповнюватись аналізом поведінки користувачів, що дозволить виявляти зловмисну діяльність на основі характеристик використовуваного трафіку та взаємодії з мережею.

Крім того, використання сигнатур для ідентифікації фроду допомагає виявляти вже відомі методи атак, тоді як аналіз поведінки користувачів та виявлення аномального трафіку дозволяють виявляти нові та невідомі методи атак.

Таким чином, комбінація різних методів моніторингу трафіку є дієвим інструментом для захисту від фроду в ip-телефонії, що забезпечує більш точний та комплексний аналіз трафіку та дозволяє виявляти як відомі, так і нові методи атак.

Література

1. https://financesonline.com/voip-software-statistics
2. https://cfca.org/
3. https://cfca.org/wp-content/uploads/2021/12/CFCA-Fraud-Loss-Survey-2021-2.pdf
4. https://www.vyopta.com/blog/business-collaboration/telecommunications-security-vulnerabilties/
5. https://www.allot.com/resources/Covid-19-Impact-Asia.pdf
6. https://www.ringcentral.com/us/en/blog/the-growing-popularity-of-voip-and-emerging-trends-in-the-market/
7. https://www.statista.com/statistics/691602/global-mobile-voip-market-size-by-region/
8. https://www.acrobits.net/blog/5g/5g-voip-global-standard/

УДК 621.396.1

ВИКОРИСТАННЯ CHAT GPT ДЛЯ ВИЗНАЧЕННЯ ПРОБЛЕМИ ПЕРЕДАЧІ ВІДЕО СИГНАЛУ ЧЕРЕЗ ПРИСТРОЇ IOT

Мєщерінов М.В.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail:mmieshch@gmail.com

USING CHAT GPT TO TROUBLESHOOT VIDEO SIGNAL TRANSMISSION THROUGH IOT DEVICES

The object of the study was the problems of video signal transmission through IoT devices using a distributed network, and the sought answer is a way to modernize the network to improve video signal transmission.

Chat GPT (Generative Pre-trained Transformer 3) - це один з найпотужніших штучно-інтелектуальних алгоритмів для генерації тексту, який був розроблений компанією OpenAI на основі технології машинного навчання. Chat GPT може генерувати текст, який виглядає, мов будь-яка людина його написала. Він може використовуватися для автоматизації процесів обробки тексту, таких як створення відповідей на запитання, генерація статей та інші завдання.

ChatGPT здатний відповісти на широкий спектр технічних запитань за умови, що вони чіткі та добре сформульовані. Ось кілька порад, частину з яких надав сам бот, які допоможуть з отриманням ефективних відповідей:

1. Будьте конкретними: уникайте розпливчастих або надто загальних запитань. Намагайтеся задавати питання, які стосуються конкретної проблеми чи теми.

2. Використовуйте правильну термінологію, але не занадто розпливчаті, або ж занадто вузько профільовані.

3. Ставлячи технічні запитання, надавайте якомога більше відповідного контексту. Це може містити інформацію про ваші поточні налаштування, проблему, яку ви намагаєтеся вирішити, і будь-які попередні спроби, які ви робили для вирішення проблеми.

4. Будьте лаконічними: постарайтеся поставити своє запитання якомога меншою кількістю слів, надаючи при цьому всю необхідну інформацію. Це допоможе ChatGPT надати більш цілеспрямовану та інформативну відповідь.

5. Краще ставити запитання англійською. Хоч і була додана українська мова до сервісу, але швидкість обробки запитів та видачі відповідей значно нижча. До того ж, після запитів українською значно більша вірогідність отримати помилку обробки запиту, яку деколи видає сервіс.

На поточному етапі розвитку, даний сервіс не може сам писати наукові роботи, не має своєї думки щодо перспектив розвитку чи використання технологій, не пропонує своїх варіантів вирішення проблем чи задач, а

всього лиш надає аналітичну чи статистичну інформацію по вже наявним проблемам, задачам та питанням. Також при зміні хоча б одного слова у запиті, чи при задаванні одного і того ж запиту через певний проміжок часу, можливі різні варіанти відповідей, так як можуть змінюватись алгоритми обробки запиту, алгоритми пошуку та обробки відповідей, база даних сервісу та інші супутні фактори. При цьому, сервіс може допомогти звузити коло пошуку інформації, надати короткий огляд суті тієї чи іншої проблеми використовуючи вже наявні матеріали. Також важливою особливістю Chat GPT є те, що він працює в форматі діалогу, тож можна розвивати тему основуючись на попередніх відповідях і запитах, тим самим поступово діставатись до суті потрібної теми.

Виконуючі дослідження, було вирішено спробувати використати Chat GPT. Об'єктом дослідження стали проблеми передачі відео сигналу через пристрої IoT використовуючи розподілену мережу, а шуканою відповіддю є спосіб модернізації мережі для покращення передачі відео сигналу. Початковим запитом було питання «Назви 5 найбільших проблем при передачі відео сигналу пристроями IoT через розподілену мережу» задля подальшого вибору шляху розвитку дослідження. У відповідь поступив наступний набір проблематик (відповіді скорочено до основних тез):

1. Обмежена пропускна здатність мережі;
2. Перевантаження мережі через передачу саме відео сигналу;
3. Зависока для передачі відео сигналу затримка мережі;
4. Перешкоди сигналу;
5. Високе енергоспоживання пристроями IoT, задіяними для передачі відеосигналу.

Задля подальшого розвитку діалогу, було розглянуто питання перевантаження мережі, а саме надіслано запит на варіанти його мінімізації, на що була отримана наступна відповідь:

1. Використання новіших методів стиснення та кодування відео, наприклад кодек H.265 (HEVC), які допоможуть значно знизити об'єм даних;
2. Реалізація методів quality of service (QoS), а саме керування смугою пропускання, приорітезація та формування трафіку;
3. Використання технології адаптивного відео бітрейту;
4. Кешування та попередня вибірка трафіку (зберігання відеовмісту, до якого часто звертаються, на локальних пристроях);
5. Розподіл трафіку між кількома стільниковими мережами.

Цього разу було отримано більш конкретні відповіді, але не всі відповіді можуть бути корисними. Наприклад, використання кодеку H.265 потребує вищих потужностей пристроїв, ніж при використанні більш звичних кодеків, але не всі пристрої інтернету речей будуть достатньо потужними. Так само реалізація технології адаптивного бітрейту. Вона допоможе в певних випадках знизити об'єми передачі інформації, але значно

збільшує навантаження на пристрій кодування та передачі сигналу, підвищуючи вимоги до їх потужності. Кешування та розподіл трафіку, хоч і знижує у певних ситуаціях об'єм переданих даних, але також підвищує навантаження на пристрої передачі та отримання даних. Розподіл трафіку між кількома мережами, наприклад двох чи трьох мобільних операторів, дійсно допоможе розвантажити мережі, але ця технологія вже широко використовується, і головне її обмеження полягає в наявності різних мереж в точці передачі. І головне, що об'єднало всі ці відповіді, що вони не допоможуть покращити мобільну мережу. Тож з п'яти відповідей, в рамках вибраної початкової цілі, лише один відповідав вибраному напрямку.

Розвиток питання QoS є актуальним і повністю підходить для подальшого розвитку мого дослідження, але через обмеження на довжину та наповненість відповідей Chat GPT, потрібно було вибрати лише один з методів реалізації QoS, і було взяте питання керування смугою пропускання. Задля перевірки можливостей, наступне питання звучало «І як керування смугою пропускання мені з цим допоможе?», на що я отримав відповідь: Приорітезації відео трафіку над іншими типами трафіку; Формування фіксованого потоку трафіку для відео даних; Розподіл смуги пропускання; Допомога в провадженні інших методів QoS.

Відповідь на це питання була досить конкретною (в порівнянні з попередніми запитами), і наблизила мене до звуження напряму дослідження. Подальших розвиток відповідей допоміг би остаточно визначитись з предметом подальшого дослідження, тобто початкову задачу Chat GPT зміг виконати.

Незважаючи на те, що для отримання конкретних відповідей і потрібної допомоги з дослідження довелось розвивати діалог від загального питання в сторону звуження відповідей, даний розмовний алгоритм може допомогти визначитись з початковою точкою наукової роботи, подальшим розвитком дослідження, допомогти розкривати потрібні питання, а також надавати список ресурсів для подальшого глибшого занурення в тему. Незважаючи на той факт, що під час написання даних тез як мова комунікації з ботом використовувалась англійська, а також бот видавав помилку генерації тексту, через що доводилось перезавантажувати сторінку, а також, на момент написання цих тез, не працювала функція збереження історії запитів, Chat GPT вже можна використовувати як помічника для пошуку інформації, і подальший його розвиток, напевно, зможе прискорити та полегшити написання наукових робіт.

Література

1 Chat GPT (Generative Pre-trained Transformer 3), 2023.

УДК 621.396.1

СКЛАДНОЩІ НАСКРІЗНОГО E2E ТЕСТУВАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Остапов О.А., Чуб М.М., Афанасьєва Л.О.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: liana.afanasyeva@gmail.com

CHALLENGES OF END-TO-END TESTING OF TELECOMMUNICATION SYSTEMS

End-to-end (E2E) network testing is critical for service providers, it helps to identify bugs early in software development process but also presents some major challenges. Testing triangle, challenges and solutions for microservices testing are presented.

Задля забезпечення сучасних потреб клієнтів, телекомунікаційні компанії впроваждують нові послуги, використовують новітні технології і постійно розширюють свою інфраструктуру. Оскільки послуги майже ніколи не бувають атомарними, а майже завжди інтегровані одна з одною, технологічні системи, що надають ці послуги - тісно пов’язані між собою. А кожен зв’язок, інтеграція однієї системи з іншою не може відбутись без детального аналізу та інтеграційного скрізного E2E тестування [1].

Для гарантування, що впроваджувані послуги - найвищої якості, QA інженерам варто розуміти основні категорії ризиків та потенційних проблем, і як насліжок - шляхи запобігання ризиків і вирішення проблем. Основні проблеми тестування телекомунікаційних системи можна розбити на категорії:

- Організаційні;
- Інфраструктурні;
- Програмні;
- Пов’язані з даними.

Організаційні ризики і проблеми, хоч і не пов’язані напряму а ні з програмним забезпеченням, а ні з апаратними комплексами, часто є одними з найсуттєвіших. Типовий приклад - розподіл необхідних прав доступів QA інженерам, коли задля задовільнення вимог департаменту безпеки, необхідні спеціалісти банально не мають змоги почати процес E2Eтестування, чи отримують його пізніше запланованого, що, відповідно, зменшує час на проведення системних інтеграційних тестів та ретест виявлених проблем. Інша типова організаційна проблема - налагодження зручних і гнучких процесів розробки і тестування. Незважаючи на декларування гнучкого підходу до проєктування (Agile) - у великих організаціях, такі як телеком компанії, багато процесів залишаються строгими, послідовними і незграбними. Більш того, в багатьох випадках до тестування ставляться як до контролю якості, тобто тест інженерів залучають запізно, в той час, як прогресивна спільнота рухається в бік QA та TestOps підходів [2].

Інфраструктурні ризики пов’язані з неточним чи несвоєчасним розгортанням необхідної інфраструктури як для процесу розробки, тестування, так і для впровадження. Не зважаючи на те, що ідеологія DevOps має вирішувати проблеми, нажаль, часто вона створює нові, такі як виділення окремих ролей для налаштування середовищ, недостатність ресурсів, нехтування тестовими середовищами, відсутність моніторингу та інженерів, що відповідають за нього

Програмні проблеми - найбільш близькі та очевидні колу QA інженерів. Сучасні розподілені системи часто базуються на мікросервісній архітектурі. Раннє тестування мікросервісів є ефективним методом виявлення помилок на початкових етапах розробки програмного забезпечення. Модифікована піраміда тестування враховує особливості контролю якості розподілених систем на мікросервісній архітектурі й включає підходи для тестування мікросервісів з нижнього рівня.

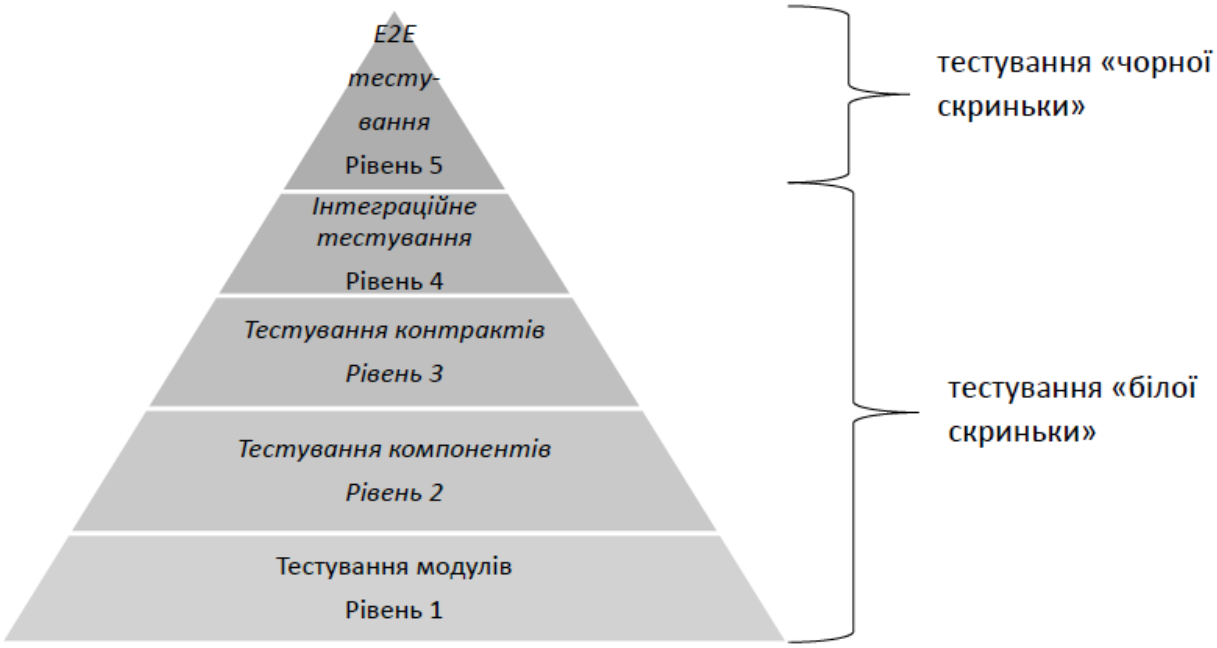


Рис.1. Трикутник тестування.

Цей підхід є частиною методології "Shift-left" у тестуванні програмного забезпечення, яка спрямована на перенесення тестування на ранні етапи розробки. Метою створення додаткових суміжних рівнів тестової піраміди для мікросервісів є виявлення різних типів проблем на початкових етапах розробки систем, що дозволяє зменшити кількість проблем в експлуатації. Кожен тип тестування спрямований на перевірку очікуваних результатів на різних рівнях програмної системи. Для розподіленої системи на мікросервісній архітектурі можна організувати тести в наступні етапи:

1. Тестування модулів - тестується невелика одиниця вихідного коду мікросервісів та перевіряєтться поведінка методів або функцій вихідного коду всередині мікросервісу, імітуючи залежні модулі та тестові дані.

2. Тестування компонентів - це тестування спрямоване на незалежне тестування всіх функціональних можливостей мікросервісів та API-інтерфейсів для окремо взятих мікросервісів.

3. Тестування контрактів - перевіряє узгоджені контракти між різними доменними мікросервісами; тестується частина інтеграції: між мікросервісом та підключеними базами даних, виклики API між двома мікросервісами.

4. Інтеграційне тестування - використовується для тестування та перевірки всієї функціональності шляхом тестування всіх пов'язаних мікросервісів.

5. E2E тестування - здійснюється наскрізне тестування функціональності системи з метою перевірки її відповідності функціональним бізнес-цілям користувача, клієнта або потенційного клієнта. E2E тестування здійснюється на зовнішньому інтерфейсі (UI) або викликах клієнта API, зокрема за допомогою REST клієнтів та проводиться в різних розподілених мікросервісах та додатках SPA/MFE. Даний вид тестування включає у себе перевірку інтерфейсу користувача, серверних мікросервісів, баз даних та їх внутрішніх/зовнішніх компонентів.

Для збільшення ефективності тестування на будь-якому етапі можна проводити тестування не з точки зору чорного ящика (QA інженер не знає, як влаштована система), а з точки зору білого ящика - включаючи перегляд вихідних кодів окремих мікросервісів, внутрішніх логів, даних в мережевих повідомленнях та записів в базах даних.

Остання, але не по значимості, категорія проблем - проблеми з даними. По-перше, в QA інженерів мають бути описи правильних і не правильних даних, які можна використовувати в інтеграційному тестуванні. По-друге, мають бути приклади самих даних. Раніше, в часи до GDPR, багато телекомунікаційних компаній використовували мінімально змінені дані зі своїх існуючих продуктових систем, оскільки ніщо не може бути кращим, ніж справжні дані. Зараз ситуація для тестування стала складніша, оскільки правильні дані для всіх мікросервісів, в потрібних кількостях потрібно генерувати самим інженерам. На їх же плечі лягає тягар забезпечення цілосності даних у випадку розподілених систем, керування даних для тестових команд і команд розробки.

Є різні підходи, від проактивних, системних, що мають на меті вирішити саму причину проблем. Власне, формулювання проблеми - вже перший крок до її вирішення, оскільки інженери часто надають перевагу не помічати очевидне. Інший підхід - реактивний - вирішення конкретних проблем по факту їх виявлення. Не зважаючи на очевидні переваги першого підходу, кожен має як переваги, так і недоліки.

Література

1. Dave Westerveld, API testing and development with postman : a practical guide to creating, testing, and managing APIs for automated software testing, 2021. – 341.
2. P. Ammann and J. Offutt, Introduction to Software Testing, Cambridge:Cambridge University Press, 201.

УДК 004.738.5

ПОРІВНЯННЯ ТРАДИЦІЙНОЇ МОДЕЛІ ВИЯВЛЕННЯ ШАХРАЙСТВА, З МАШИННИМ НАВЧАННЯМ

Міночкін Д. А., Кошмак А.І.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: dmytro.minochkin@gmail.com , koshmak02@gmail.com

COMPARISON OF TRADITIONAL FRAUD DETECTION MODEL WITH MACHINE LEARNING

The article analyzes machine learning, its methods, advantages and disadvantages, combating fraud.

Шахрайство в мережі є серйозною проблемою, від якої страждають люди. Воно передбачає несанкціоноване використання, втручання або маніпуляції з мобільним телефоном або особистими даними, з метою незаконного отримання грошей. Шахраї можуть використовувати різні вразливі місця та лазівки в інфраструктурі мобільних мереж, пристроях і послугах для здійснення своїх зловмисних дій. Машинне навчання стає все більш популярним у боротьбі з цим. За допомогою цієї технології можна виявляти шахраїв та уникати фінансових втрат [1].

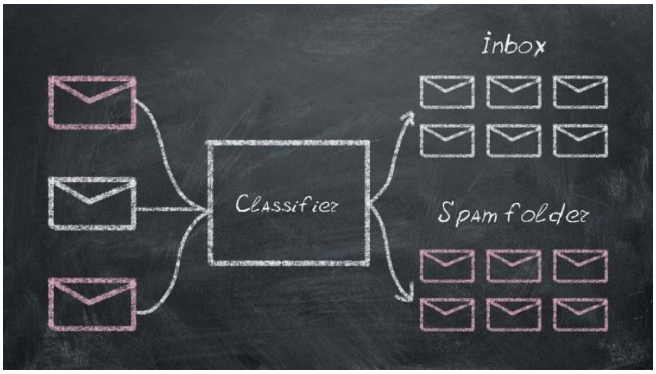
Історія розвитку машинного навчання виявлення шахрайства почалася в 1990-х роках, коли комп'ютерна технологія стала досить розвиненою, щоб обробляти велику кількість даних та виконувати складні завдання. Початково машинне навчання застосовувалось для виявлення шахрайства в фінансових транзакціях, але згодом воно стало застосовуватись в багатьох інших сферах, таких як медицина, транспорт, торгівля та інші.

У 2000-х роках машинне навчання почало розвиватись з використанням глибокого навчання, що дало можливість створювати більш точні та надійні моделі виявлення шахрайства. Глибоке навчання дозволяє навчити комп'ютер розпізнавати складні залежності між різними ознаками транзакцій та виявляти навіть найскладніші форми шахрайства.

Сьогодні машинне навчання стало необхідністю для багатьох організацій, які працюють з великою кількістю даних та проводять транзакції в Інтернеті. Воно дозволяє автоматизувати процес виявлення шахрайства та зменшити кількість помилок, що можуть бути зроблені людським фактором. Крім того, здатне швидко виявляти нові форми шахрайства, які можуть виникнути в майбутньому, що дозволяє забезпечити більш ефективне захист від шахрайства [2].

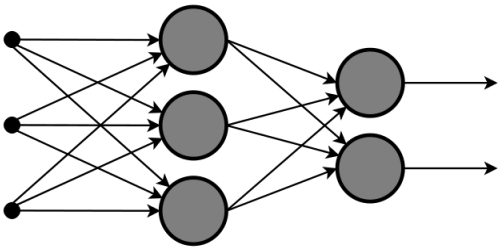
Машинне навчання є кращим для визначення шахрайства в порівнянні з іншими методами. Ось основні методи машинного навчання для виявлення шахрайства:

Класифікація: цей метод полягає в тому, щоб навчити комп'ютер розпізнавати шаблони шахрайства на основі історичних даних та використовувати їх для виявлення нових випадків. Цей метод зазвичай використовується для виявлення фішингових атак, коли шахраї відправляють листи, щоб перехопити особисту інформацію.



Кластеризація: цей метод полягає в тому, щоб навчити комп'ютер групувати схожі транзакції за специфічними ознаками, такими як місцезнаходження або час. Якщо певний клас транзакцій виявляється як шахрайство, то можна більш ефективно виявляти подібні шаблони шахрайства у майбутньому.

Нейронні мережі: цей метод полягає в тому, щоб навчити комп'ютер розпізнавати складні зв'язки між різними ознаками транзакції. Це дає можливість виявляти більш складні форми шахрайства, такі як використання штучного інтелекту.



Методи класифікації, кластеризації та нейронних мереж дозволяють автоматизувати процес виявлення шахрайства та зменшити кількість помилок, які можуть виникнути в результаті ручного аналізу. Проте, успішне використання машинного навчання в сфері виявлення шахрайства потребує

якісних даних, а також постійного оновлення навчальних моделей для забезпечення ефективного виявлення найновіших форм шахрайства.

Машинне навчання має кілька переваг в порівнянні з традиційними методами. Ось деякі з них:

Відсутність людського фактору: Комп'ютерні алгоритми, навчені на підставі історичних даних, можуть бути більш точними та ефективними виявляти шахрайство, оскільки не піддаються людському впливу.

Швидкість та ефективність: Машинне навчання може обробляти великі обсяги даних в значно менші терміни, порівняно з людськими аналітиками. Це дозволяє виявляти шахрайство швидше та з меншою кількістю помилок.

Автоматизація: Машинне навчання може бути повністю автоматизованою системою, що дозволяє виявляти шахрайство в режимі реального часу. Це дозволяє реагувати на шахрайство швидко та ефективно, тим самим запобігаючи великій кількості втрат.

Спроможність адаптуватися: Машинне навчання може адаптуватися до нових форм шахрайства, що постійно з'являються. Це дозволяє підтримувати високий рівень ефективності при виявленні шахрайства, незалежно від того, наскільки складним воно може бути. [3]

Традиційна модель виявлення шахрайства, яка базується на статичній системі, на основі правил, має свої переваги та недоліки. Основна перевага полягає у тому, що правила відображають досвід та знання експертів, тому вони можуть бути досить ефективними виявляти підозрілу активність в мережі. Однак, ці системи мають кілька значних недоліків.

По-перше, статична система на основі правил сильно залежить від людської праці. Навіть якщо правила розробляють найкращі експерти, це все одно обмежує можливості системи, оскільки вона не може адаптуватися до нових видів шахрайства та інших змін у мережі. По-друге, створення та вдосконалення правил потребує часу та зусиль. Нові види шахрайства постійно з'являються, тому статична система на основі правил не завжди може бути вчасно оновлена, щоб виявляти нові загрози. По-третє, статична система може бути досить складною та містити велику кількість правил, що може ускладнювати її підтримку та розуміння сторонніми користувачами.

В цілому, традиційна модель може бути корисною, але її обмеженості та недоліки можуть бути проблемою для ефективного виявлення шахрайства в сучасних цифрових середовищах.

Виявлення шахрайства за допомогою машинного навчання може вирішити всі ці проблеми. Навіть перевершити традиційні системи виявлення шахрайства за швидкістю, якістю та економічною ефективністю.

Література

1. C. M. Bishop. Pattern Recognition and Machine Learning. Springer, 2006.
2. Hiyam, A. E. Tawashi, Detecting Fraud in Cellular Telephone Networks Jawwal Case Study. MBA thesis Islamic University, Faculty of Commerce, Department of Business Administration, Gaza. 2010.
3. Bolton, R. J. and Hand, D. J., Statistical Fraud Detection, A review, Institute of Mathematical Statistics, 2002. 17(3).

УДК 621.384.3

ВИКОРИСТАННЯ ПРОТОКОЛУ ZIGBEE В БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖАХ: РОЗРОБКА JAVA ДОДАТКУ ДЛЯ МОНІТОРИНГУ ПРИСТРОЇВ НА ОСНОВІ ZIGBEE

Руренко О.Г., Денищич Н.М.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: a.rurenko@gmail.com , nadyadenishich@gmail.com

USING THE ZIGBEE PROTOCOL IN WIRELESS SENSOR NETWORKS: DEVELOPMENT OF A JAVA APPLICATION FOR MONITORING ZIGBEE-BASED DEVICES

Educational and Scientific Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine E-mail: a.rurenko@gmail.com , nadyadenishich@gmail.com

The article describes the Zigbee pipeline and the XBee library, which is used to develop a Java application for device monitoring.

У статті описано протокол Zigbee та бібліотеку XBee, за допомогою якої відбувається розробка Java-додатку для моніторингу пристроїв.

Останнім часом дуже сильно зростає популярність технологій бездротових сенсорних мереж, які використовуються для збору даних у різних галузях, таких як медицина, промисловість, будівництво та інші. Протоколи бездротового зв’язку в сенсорних мережах відіграють ключову роль у забезпеченні ефективної роботи та надійної комунікації між вузлами.

Оскільки сенсорні мережі мають обмежені ресурси, такі як обмежена енергопотреба, обмежена швидкість передачі даних, вони потребують протоколів, які б дозволяли ефективно використовувати ці ресурси та забезпечували мінімальний рівень помилок при передачі даних.

Використання протоколу Zigbee у бездротових сенсорних мережах дозволяє забезпечити стійку та надійну комунікацію на відстань до 10 км з високою енергоефективністю.

ZigBee — це протокол бездротового зв’язку, який успішно використовується в різноманітних додатках від домашньої автоматизації до промислового керування та споживчої електроніки.

Він особливо підходить для бездротових сенсорних мереж через низьку вартість пристроїв і їх низьке енергоспоживання. ZigBee працює вище стандарту бездротового зв’язку IEEE 802.15.4, який містить процедури доступу до середовища та фізичного рівня для забезпечення роботи в неліцензійному частотному спектрі. Додатковою перевагою протоколу

ZigBee є його здатність розширювати дальність зв'язку за допомогою багатопрохідного зв'язку.

ZigBee відрізняється від таких протоколів, як IEEE 802.11, тим, що він визначає використання повного набору протоколів, спеціально розроблених для зв'язку між пристроями.

На рівні додатків ZigBee визначає профілі додатків, які полегшують зв'язокміж додатками на різних пристроях, а також визначають процедури для виявлення мережі та встановлення з'єднання. ZigBee також визначає підрівень підтримки додатків (APS), який керує поточними з'єднаннями та має функції транспортного рівня для наскрізної надійної передачі даних із підтвердженнями, повторними передачами та відхиленням дублікатів пакетів.

На своєму мережевому рівні ZigBee визначає процедури для встановлення маршрутів зв'язку з кількома переходами між пристроями, визначаючи процедури для виявлення маршруту та алгоритми маршрутизації. Визначено чотири алгоритми маршрутизації: маршрутизація на основі таблиці (схожа на AODV), маршрутизація ієрархічного дерева, багатоадресна маршрутизація та багато-до-одного маршрутизація джерела.

Для підтримки мережевих функцій ZigBee також визначає, що вузли періодично транслюють повідомлення про стан зв'язку (LS). У кожному повідомленні LS вузол транслює своє поточне уявлення про кожне сусіднє посилання. Точніше, повідомлення LS, передане вузлом, містить список усіх сусідів вузла та містить вартість зв'язку від кожного з його сусідів до вузла.

Важливо підкреслити:

- Вартість зв'язку, наявна в повідомленні LS, квантується у три біти.

- ZigBee розрізняє вартість вихідного та вхідного зв'язку; однак для маршрутизації M2O специфікації ZigBee визначають, що вартість шляху базується на максимумі між ними. Щоб спростити наше обговорення, витрати на посилання в цій статті стосуються максимуму між вхідними та вихідними витратами на посилання.

Програма Java для моніторингу пристроїв Zigbee:

Для моніторингу пристроїв Zigbee можна розробити програму Java за допомогою бібліотеки XBee.

Бібліотека XBee Java — це API Java, який значно скорочує час виходу на ринок проектів XBee, розроблених на Java, і полегшує розробку таких типів програм, роблячи цей процес легким і плавним. Бібліотека XBee Java містить такі функції:

- Підтримка кількох пристроїв і протоколів XBee.

- Високий рівень абстракції забезпечує простий у використанні робочий процес.

- Можливість налаштування локальних і віддалених пристроїв XBee мережі.

- Функція виявлення знаходить віддалені вузли в тій же мережі, що й локальний модуль.

- Можливість передачі та отримання даних з будь-якого пристрою XBee в мережі.

- Можливість керувати вхідними та вихідними лініями загального призначення всіх ваших пристроїв XBee.

- Можливість надсилати та отримувати дані між локальними інтерфейсами XBee (Bluetooth Low Energy, MicroPython і Serial Port).

Бібліотека XBee Java також пропонує підбібліотеку для розробки додатків Android, які керують пристроями XBee або спілкуються з ними через Bluetooth Low Energy, USB або послідовний порт. Ця документація допоможе вам на різних етапах розробки ваших програм Java або Android з використанням цих бібліотек.

Отже, Zigbee є важливим протоколом бездротового зв'язку для бездротових сенсорних мереж. Він забезпечує протокол зв'язку з низьким енергоспоживанням і низькою швидкістю передачі даних, який ідеально підходить для моніторингу фізичних параметрів. Завдяки бібліотеці XBee можна розробити програму Java для моніторингу пристроїв Zigbee у мережі.

Література

1. Ludovici A., Calveras A., Casademont J. Forwarding techniques for IP fragmented packets in a real 6LoWPAN network. Sensors. 2011;11:992–1008 [Електронний ресурс] – Режим доступу до ресурсу: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3274068/.
2. Gomez C., Paradells J. Wireless home automation networks: A survey of architectures and technologies. IEEE Commun. Mag. 2010;48:92–101.
3. Specification of the Bluetooth System, Covered Core Package, Version: 4.0. The Bluetooth Special Interest Group; Kirkland, WA, USA: 2010.
4. Ns-3: A Discrete-Event Network Simulator for Internet Systems. [(accessed on 1 December 2019)];2019 Available online: https://www.nsnam.org.
5. Chang K.-M., Liu S.-H., Wu X.-H. A Wireless sEMG recording system and its application to muscle fatigue detection. Sensors. 2012;12:489–499.
6. Chang K.-M., Liu S.-H., Wu X.-H. A Wireless sEMG recording system and its application to muscle fatigue detection. [Електронний ресурс] – Режим доступу до ресурсу: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3279225/.

УДК 004.94

ОНТОЛОГІЧНЕ МОДЕЛЮВАННЯ ТЕХНОЛОГІЧНИХ ПРОЦЕСІВ ДЛЯ ВИРОБНИЦТВА ДЕТАЛЕЙ СКЛАДНОЇ ФОРМИ

[1]Глоба Л.С., [1]Новогрудська Р.Л., [2]Копійка О.В.
[1] *Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна*
[2]*Інститут телекомунікацій і глобального інформаційного простору Національної академії наук, Україна*
E-mail: lgloba@its.kpi.ua, rinan@ukr.net, kopiika@nas.gov.ua

ONTOLOGICAL MODELING OF TECHNOLOGICAL PROCESSES FOR THE PRODUCTION OF DETAILS OF COMPLEX FORM

The research proposes an original approach to the design and storage of data and knowledge regarding objects of technological process for end-production preparation (parts, equipment, materials, design procedures, etc.). It is involved to use ontological model for modelling the technology of manufacturing complex details.

На сьогоднішній день термін «знання» розглядається з різних точок зору [1]. Одна з них, позиціонує знання як умову доступу до інформації. Стверджується, що представлення знань повинно бути організоване таким чином, щоб до них було легко отримати доступ та отримати їх.

У джерелі [2] стверджується, що представлення знань вимагає різних стратегій та різних видів інструментів та технологій для управління знаннями. Наприклад, якщо знання розглядаються як об'єкт, то ініціативи управління знаннями повинні підкреслювати важливість створення запасів знань в організаціях. У цьому випадку система управління знаннями така, як сховища знань, повинна мати здатність фіксувати запаси знань. Аналогічним чином, якщо знання розглядаються як процес, то ініціативи з управління знаннями повинні оперувати з потоками знань у процесах створення знань, обміну знаннями та поширенні знань.

На сьогоднішній день існують різні моделі представлення знань [3, 4], кожна з яких має свої переваги та недоліки. Онтологічне моделювання є одним з найчастіше використовуваних способів представлення знань на поточний момент [5] оскільки дозволяє не лише структурувати та систематизувати знання, але і описати певні процеси взаємодії між даними для видобутку нових знань.

Для автоматизації виробничих та технічних процесів на поточний момент використовуються різні SAP системи та технології опису бізнес процесів та workflow. Однак, для коректного менеджменту сучасних робочих процесів дуже важливо також враховувати компоненти управління та

представлення знань, які використовуються та генеруються під час виконання таких виробничих процесів.

Наведене дослідження присвячене розробці онтології, яка характеризує виробничий технологічний процес. Така отологія представляє собою систему взаємозв'язаних компонент, кожна з яких є завершеною онтологією сама по собі, а у сукупності множина таких компонент дозволяє не лише описати усі елементи та стадії технічного процесу, але і відповідне обладнання, програмне та технічне забезпечення яке використовується у технічному процесі, а також ввести та описати деякі показники ефективності описуваного технологічного процесу. Систему антологій для опису технічного процесу представлено на рис. 1.

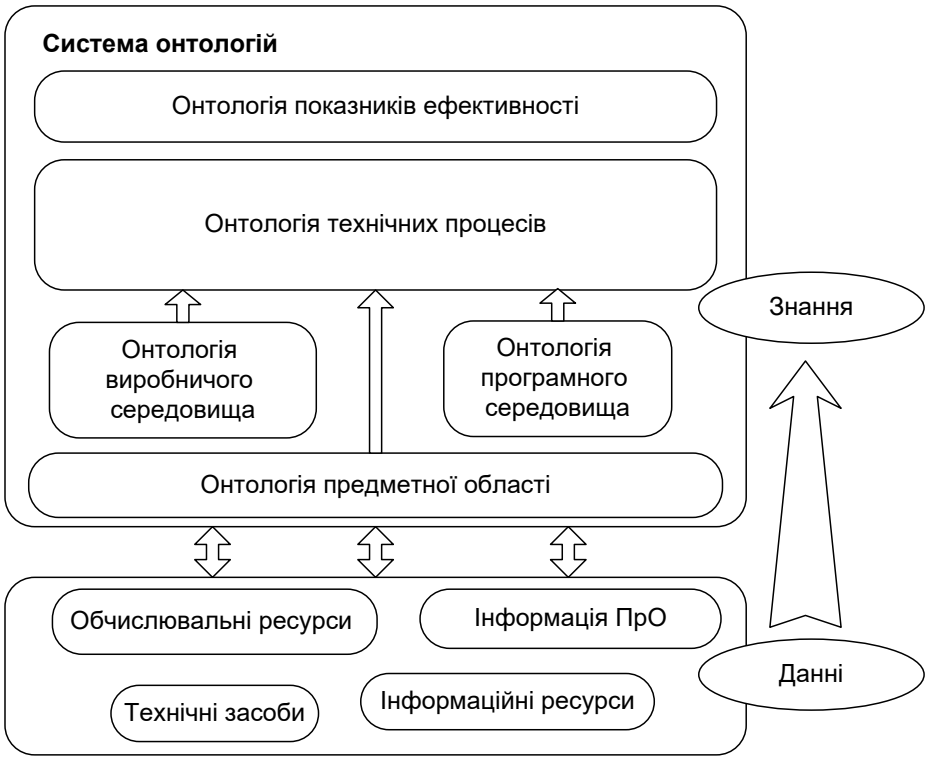


Рис. 1. Система онтологій для опису технологічного процесу.

Онтологія технічних процесів є основною онтологією системи, вона описує характеристики та елементи технологічного процесу, а також зв'язки між ними. В систему включено три онтології нижнього рівня: Онтологію виробничого середовища, онтологію програмного забезпечення та онтологію предметної області. Онтологія виробничого середовища описує різноманітні технологічні засоби, такі як обладнання, устаткування, інструменти та матеріали, які використовуються у технологічному процесі; Онтологія програмного середовища описує програмне забезпечення та технічні засоби які використовуються у технічному процесі; Онтологія предметної області базується на безпосередньому описі концептів предметної області та задає структури для їх «поєднання» з іншими онтологіями системи, вона містить усю інформацію яка стосується процесів та об'єктів які приймають участь у

технічному процесі, в залежності від того для якої предметної області відбувається цей технологічний процес.

В процесі побудови кожної з введених онтологій необхідно описати її елементи. Онтологія включає наступні елементи: класи, атрибути, відношення, типи значень атрибутів, обмеження на значення атрибутів, екземпляри класів.

Саме така множина елементів дозволяє задати онтологію як комплексну модель. Таким чином, онтологія являє собою ієрархію понять (або класів), пов'язаних відношеннями. Використання відношень асоціативного типу дозволяє визначити онтологічну модель не тільки як ієрархічну структуру, але і як структуру, що враховує змістовний сенс зв'язку між реальними об’єктами. Різні властивості кожного поняття описуються на основі атрибутів понять і обмежень, накладених на область їх значень.

Онтологія технологічного процесу містить множину класів, які описуються відповідними атрибутами. Класи – це елемент онтологічної моделі, який описує поняття деякої предметної або проблемної області. Атрибути – елементи онтологічної моделі, які описують властивості класів і відношень. Типи значень атрибутів задають стандартні типи для значень атрибутів класів (наприклад: string, integer, real, date). Обмеження на значення атрибутів класів та відношень використовується не для всіх атрибутів, а лише для тих, значення яких повинні лежати в деякій області, не можуть бути менше/більше заданої величини або визначаються певним правилом.

Запропонований у дослідженні підхід до представлення елементів технологічного процесу у вигляді онтологічної моделі дозволяє отримати функціонально повний перелік елементарних, алгоритмічно коректних функціональних задач, призначених для проектування документів конструкторсько-технологічної підготовки виробництва; методів прийняття технічних рішень з використанням штучного інтелекту; принципів гнучкої адаптації до конкретного виробничого середовища та вимог сучасного ринку.

Література

1. Davis, Randall & Shrobe, Howard & Szolovits, Peter. (2002). What Is a Knowledge Representation?. AI Magazine. 14., P. 17-33.
2. Alavi, M. and Leidner, D., (2001) Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues. MIS Quarterly, 25(6), 95-116.
3. Kavitska, Viktoriia & Liubchenko, Vira & Lysyuk, A.. (2013). A knowledge representation model for knowledge management systems. Odes’kyi Politechnichnyi Universytet. Pratsi. 167-172. 10.15276/opu.3.42.2013.33.
4. Tanwar, Poonam & Prasad, T. & Dutt, Kamlesh. (2018). A Tour Towards the Various Knowledge Representation Techniques for Cognitive Hybrid Sentence Modeling and Analyzer. International Journal of Informatics and Communication Technology (IJ-ICT). 7. 124. 10.11591/ijict.v7i3.pp124-134.
5. Globa L.S., Gvozdetska N.A., Novogrudska R.L., Ontological model for data processing organization in information and communication networks (2021) System Research and Information Technologies, 2021 (1), pp. 47 - 60, DOI: 10.20535/SRIT.2308-8893.2021.1.04].

УДК 004.94

РОЗРОБКА МЕТОДУ ДИНАМІЧНОГО КЕРУВАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЮ ІНФРАСТРУКТУРОЮ

Пархоменко Д.О., Скулиш М.А.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: parhomas98@gmail.com

DEVELOPMENT OF A METHOD OF DYNAMIC MANAGEMENT OF INFORMATION AND COMMUNICATION INFRASTRUCTURE

The main directions of the principle of operation of the hypervisor in SDN are summarized. The results of the analysis of ensuring the criteria for the functioning of the information and communication network for existing hypervisor solutions are given.

Програмно–конфігурована мережа (SDN, Software-defined Networking) - мережа передачі даних, в якій рівень управління мережею відділений від пристроїв передачі даних і реалізується програмно [1]. SDN – це нова концепція, яка має на меті зняти функції площини управління з мережевих пристроїв і розмістити їх у спеціалізованому, логічно централізованому контролері мережі. Це дає перевагу в спрощенні конфігурації мережі та дотримання правил. Це також зменшує необхідні системні ресурси, оскільки вони більше не потрібні для запуску функцій площини управління [2].

Зараз постачальники послуг віртуалізують частини своєї мережі. Такий підхід істотно впливає на рішення для аналізу та оцінки параметрів продуктивності, що використовуються для забезпечення роботи мережі. Продуктивність нових мереж істотно залежить від організації обчислювального процесу в системах, що забезпечують їх функціонування. Планування роботи віртуалізованої мережі, яка забезпечує обслуговування гібридних інформаційно-телекомунікаційних послуг, забезпечує умовно нескінченний обчислювальний ресурс [2].

Експерименти проводяться на, віртуальному тестовому стенді на основі Mininet [3] для оцінки функціональних аспектів віртуалізації мережі.У всіх експериментах контролером OpenFlow використовується Floodlight [4], оскільки це простий у налаштуванні контролер і містить усі функції, необхідні для експерименту з тестованими мережами.

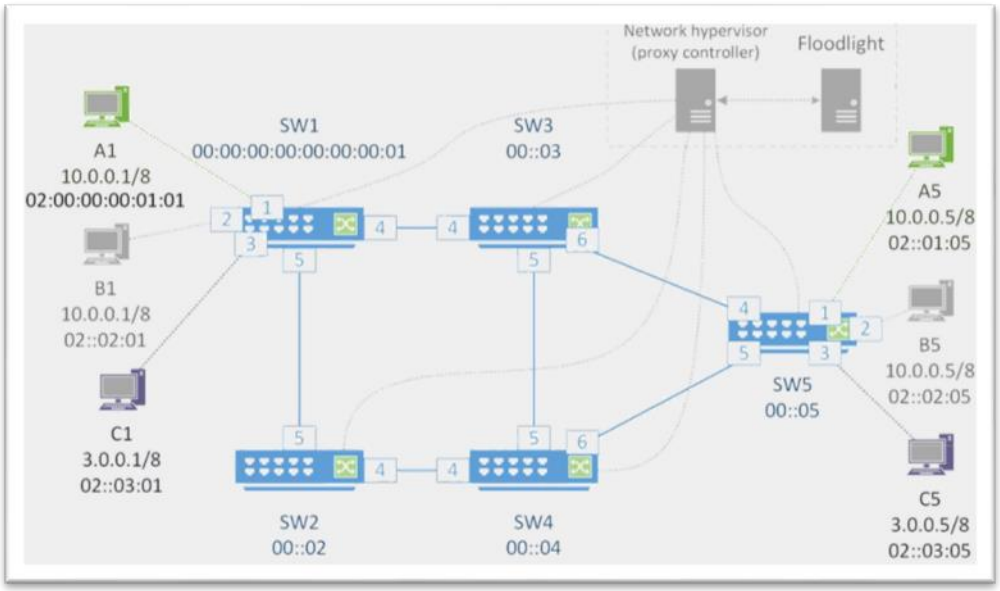


Рис.1. Тестовий сценарій Mininet.

Графічний інтерфейс Floodlight був використаний для перевірки того, що гіпервізори мережі виставляли правильне подання віртуальної мережі контролерам оренди. Три екземпляри контролера орендаря Floodlight були створені в портах 10000, 20000 та 30000 для управління мережами A, B та C відповідно. Ізоляція мережі також була перевірена з точки зору мережевих хостів.

Таблиця 1. Підключення хостів, в

	A1	A2	A3	A4	A5	B1	B2	B3	B4	B5	C1	C2	C3	C4	C5
A1	–	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N
A2	Y	–	Y	Y	Y	N	N	N	N	N	N	N	N	N	N
A3	Y	Y	–	Y	Y	N	N	N	N	N	N	N	N	N	N
A4	Y	Y	Y	–	Y	N	N	N	N	N	N	N	N	N	N
A5	Y	Y	Y	Y	–	N	N	N	N	N	N	N	N	N	N
B1	N	N	N	N	N	–	Y	Y	Y	Y	N	N	N	N	N
B2	N	N	N	N	N	Y	–	Y	Y	Y	N	N	N	N	N
B3	N	N	N	N	N	Y	Y	–	Y	Y	N	N	N	N	N
B4	N	N	N	N	N	Y	Y	Y	–	Y	N	N	N	N	N
B5	N	N	N	N	N	Y	Y	Y	Y	–	N	N	N	N	N
C1	N	N	N	N	N	N	N	N	N	N	–	Y	Y	Y	Y
C2	N	N	N	N	N	N	N	N	N	N	Y	–	Y	Y	Y
C3	N	N	N	N	N	N	N	N	N	N	Y	Y	–	Y	Y
C4	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	–	Y
C5	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	–

Mininet.

За допомогою інструменту test_packets.py було перевірено багато типів трафіку, щоб оцінити, чи блокують контролери віртуалізації певні кадри. Узагальнені результати наведені в таблиці та класифіковані на шість різних категорій.

Type of traffic	L2	OVS	FL	FV	OV
IPv4 unicast	+	+	+	+	+
IPv6 unicast	+	+	+	-	-
IPv4 multicast	+	+	+	+	+
L2 multicast	+-	-	+-	+-	+-
IPv4 w/ VLAN	+	+	+	+	+
IPv4 w/ MPLS	+	+	+	+	+

Таблиця 2. Узагальнені результати пересилання трафіку.

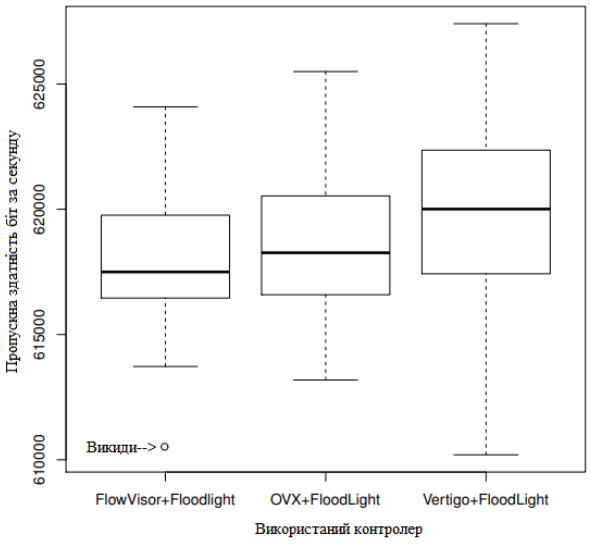


Рис.2 Пропускна здатність, виміряна різними контролерами в бітах за секунду.

Загалом, перевірені мережеві гіпервізори напрочуд добре передавали кілька типів трафіку. Єдині загальні проблеми, що спостерігаються, трапляються з трафіком IPv6, LLDP та STP. IPv6 не підтримується OpenFlow 1.0, який використовується як OVX, так і FlowVisor.

Тест пропускної здатності базується на iperf в режимі TCP. TCP являється найкращим протоколом, і пропускна здатність залежить від затримки мережі, розміру кадру, втрати пакетів, міжкадрового розриву та інших мережевих умов.

Результати експериментів, проведених у фізичній топології, зведені на рисунку 2. Пропускна здатність із FlowVisor в середньому становить 617,9 кбіт / с, OVX 618,6 кбіт / с та VeRTIGO 620,0 кбіт / с. Однак дисперсія у всіх результатах досить велика, і статистично не спостерігається значної різниці в отриманій смузі пропускання, виміряній між двома хостами при переході на різні гіпервізори мережі.

На основі спостережень, зроблених протягом цієї роботи, FlowVisor найкраще підходить для роботи з різними програмами в рамках однієї мережі. Він може бути використаний як засіб віртуалізації мережі, щоб дозволити різним клієнтам спільно використовувати ресурси переадресації рівня 2, забезпечуючи ізоляцію між зрізами.

Література

1. SDN&NFV / Bellintegrator: Режим доступу: http://www.bellintegrator.ru/services-sdn-nfv.html
2. Барсков А. SDN: кому и зачем это надо?/ Журнал сетевых решений/LAN. 2012. № 12. –. – Режим доступу: https://www.osp.ru/ lan/2012/12/13033012
3. Mininet. (Feb. 2016). Mininet overview, [Online]. Available: http://mininet.org/ overview/ (visited on 01/20/2016).
4. F. Pakzad, M. Portmann, W. L. Tan, and J. Indulska, “Efficient topology discovery in software defined networks,” in Signal Processing and Communication Systems (ICSPCS), 2014 8th International Conference on, Dec. 2014, pp. 1–8. doi: 10.1109/ICSPCS.2014.7021050

UDC 004.056.53

EFFICIENCY OF USER AUTHENTICATION METHODS IN MOBILE NETWORKS

Forostianko K.Y., AstrakhantsevA.A.
Educational and Scientific Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: forostiankokarina@gmail.com, aastrakhantsev@its.kpi.ua

ЕФЕКТИВНІСТЬ МЕТОДІВ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ В МОБІЛЬНИХ МЕРЕЖАХ

Віддалена автентифікація користувачів у мобільних мережах 4G/5G є ключовим елементом забезпечення безпеки в мережах зв'язку. Однак, з огляду на швидкий розвиток технологій та зростання кількості підключених пристроїв, необхідно вдосконалювати методи автентифікації для забезпечення максимальної захищеності. У цій роботі проаналізовані характеристики способів віддаленої біометричної автентифікації користувачів в мобільних мережах і визначений найбільш ефективний за сукупністю критеріїв.

Remote authentication of users in mobile networks is a key element of ensuring security in communication networks. However, given the rapid development of technology and the growing number of connected devices, it is necessary to improve authentication methods to ensure maximum security. This article will analyze various methods of providing remote user authentication in mobile networks.

The threat of attacks on mobile networks and online payment systems is real, and the need for protection has become more pressing than ever. To address these challenges, biometric authentication has emerged as a promising solution for remote authentication. Biometric authentication uses a person's unique biological characteristics to verify their identity. This type of authentication is much more secure than traditional password-based systems, which can easily be compromised by hackers.

The purpose of implementing biometric authentication in mobile networks and online payment systems is to provide users with a higher level of security and to reduce the risk of fraud and other security threats. By using biometric authentication, businesses and individuals can ensure that only authorized users have access to sensitive information and transactions. There are several biometric authentication methods that are suitable for mobile devices, including:

- *Fingerprint recognition.* This method is one of the most commonly used biometric authentication methods on mobile devices. It works by scanning the user's fingerprint to verify their identity.
- *Facial recognition.* This method uses the front-facing camera of a mobile device to capture and analyze the user's facial features. It is becoming increasingly popular on mobile devices due to its ease of use.

- *Iris recognition.* This method uses the unique patterns of the user's iris to verify their identity. It requires specialized hardware and is not as widely available as other methods.
- *Voice recognition.* This method uses the user's voice to verify their identity. It can be used for speaker verification or speaker identification.

When comparing different biometric authentication methods for mobile devices, several characteristics should be considered. These include:

– Universality: This refers to the percentage of the population that can use the biometric method.

– Uniqueness: This refers to the degree of distinctiveness of the biometric trait.

– Permanence: This refers to the stability of the biometric trait over time.

– Performance: This refers to the accuracy and speed of the biometric method.

– Acceptability: This refers to the level of comfort and ease of use of the biometric method by users.

– Ease of use: This refers to the simplicity and convenience of the biometric method for users.

– Long-term stability: This refers to the ability of the biometric method to maintain its accuracy and reliability over an extended period of time.

Table 1. Comparison of biometric identification methods.

Biometric	Universality	Uniqueness	Permanence	Performance	Acceptability	Ease of use
Face	High	Low	Medium	Low	Medium	Medium
Fingerprint	Medium	High	High	High	Medium	High
Hand geometry	Medium	Medium	Medium	Medium	Medium	High
Iris Scanning	High	High	High	High	Medium	Medium
Retinal Scanning	High	High	Medium	High	Medium	Low
Voice Recognition	Medium	Low	Low	Low	High	High
Signature	Low	Low	Low	Low	High	High
Hand Vein	Medium	Medium	Medium	Medium	Medium	Medium
DNA	High	High	High	Low	Low	Medium

When making decisions about choosing the best option for a biometric authentication system, it is necessary to determine the importance (priority) of the requirements that apply to the parameters of the biometric authentication system. Algorithms of comparison methods are similar, but if there are differences between them, different criteria for the importance of criteria can be given, which in time can lead to obtaining an incorrect result. Another problem is the degree of

consistency of experts' assessments. In the methods of pairwise comparison (tab. 1), the expert expresses his opinion about the ratio of importance of all possible pairs of criteria in the form of intensity of relative importance, which is quantified using a scale of relative importance. The relative degree of superiority (dominance) of one criterion over another is set by the expert based on his knowledge of the real processes that take place in the nodes of the system with biometric characteristics of a person, that is, this quantitative assessment is subjective. Therefore, the vector of priority coefficients will depend on the number of experts and the level of their experience and qualifications.

According to the method of pairwise comparisons, table 1 was modified to the numeric form and based on it, the best methods was defined. The result showed in table 2:

Table 2. Result of comparisons.

Face	10,3
Fingerprint	**13**
Hand geometry	8,8
Iris Scanning	**11,4**
Retinal Scanning	8,4
Voice Recognition	8,2
Signature	7,3
Hand Vein	7,5
DNA	9,8

Conclusion. According to the results, showed in tab.2, the best biometric authentication method for remote authentication via mobile device would be a fingerprint scan. This method gives the highest result for the criteria listed above and can be recommended for use in mobile networks. The iris method also provides good value and can be used as additional way or for multifactor authentication.

References

1. Private eyes: Secure remote biometric authentication: Ewa Syta; Michael J. Fischer; David Wolinsky; Abraham Silberschatz; Gina Gallegos-García; Bryan Ford. Published in: 2015 12th International Joint Conference on e-Business and Telecommunications (ICETE).
2. A Remote Biometric Authentication Protocol For On-Line Banking: Anongporn Salaiwarakul. DOI: 10.5769/C2013002 OR HTTP://DX.DOI.ORG/10.5769/C2013002.
3. Chen, L., Pearson, S., Vamvakas, A.: Trusted Biometric System. Available at URL http://www.hpl.hp.com/techreports/2002/HPL-2002- 185.pdf (2002).
4. Salaiwarakul, A., Ryan, M.: Analysis of a Biometric Authentication Protocol for Signature Creation Application. Third International Workshop on Security (2008) 231-245.

UDC 004.75

STUDY OF THE EFFICIENCY OF MACHINE LEARNING ALGORITHMS FOR TRAFFIC CLASSIFICATION IN MOBILE NETWORKS

Sushko O.V., Astrakhantsev A.A.
Educational and Scientific Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: aastrakhantsev@its.kpi.ua, sushko.oleksandra@gmail.com

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ КЛАСИФІКАЦІЇ ТРАФІКА В МОБІЛЬНИХ МЕРЕЖАХ

У статті ставиться актуальне завдання аналізу ефективності алгоритмів машинного навчання для вирішення завдання класифікації трафіка в мобільних мережах у режимі реального часу. Для досягнення мети аналізується точність класифікації та швидкодія для найпоширеніших алгоритмів машинного навчання та визначається оптимальний алгоритм за критерієм точності класифікації. Окрім цього, у статті виконано оцінку важливості полів датасету для класифікації трафіка.

The article presents the actual task of analyzing the effectiveness of machine learning algorithms to solve the task of traffic classification in mobile networks in real time. To achieve the goal, the classification accuracy and speed of the most common machine learning algorithms are analyzed and the optimal algorithm is determined based on the criterion of classification accuracy. In addition, the article evaluates the importance of dataset fields for classification.

Classification of network traffic can be carried out based on the use of information from different levels of the OSI (Open Systems Interconnection) model. At the physical layer, analysis and classification can be performed based on bit sequences and volume traffic [1]. At higher levels, port numbers, packet contents, flow identifiers, and packet headers can be used for this. At the same time, the characteristics of network traffic at each of the levels differ. For example, at the packet flow level, network traffic is characterized by packet size and the time interval between packets. Analysis at the bit sequence level mainly concerns such characteristics as transmission intensity and channel bandwidth. At the packet flow level, the procedure for the arrival of IP packets, i.e. their delay and loss, is also considered.

In many works, such algorithms as random forest (RF), KNN, ANN and SVM are proposed for use. Therefore, these algorithms were chosen for research in this work. In addition to machine learning algorithms for traffic classification, Deep Packet Inspection (DPI) methods also can be used. Deep Packet Inspection is the most advanced technology for traffic classification because it is the most accurate technique [2]. Therefore, often the most popular products, both commercial and open source, rely on DPI when classifying traffic. However, the

actual effectiveness of DPI is still uncertain, as the limited number of public datasets limits the comparison and reproducibility of results [3].

Now let's move on to the analysis of features for traffic classification. Consider the packet fields given in the dataset that can be used as features for model training and traffic classification. A short list of fields is given in the table 1.

Table 1. List of fields for traffic classification.

Flow ID	Flow Duration	Flow bytes/s	Average Packet Size
Source IP	Total Fwd Packets	Flow packets/s	Avg Fwd Segm Size
Source Port	Total Backward Packets	Average Packet Size	Avg Bwd Segm Size
Destination IP	Total Length of Fwd Pck	Flags (x 8)	Fwd Header Length
Destination Port	Total Length of Bwd Pck	Packet Length Mean	Down Up Ratio
Protocol	Fwd Packet Length Max	Bwd Packet Length Max	Label
Timestamp	Fwd Packet Length Min	Bwd Packet Length Min	App name

As can be seen from the table. 1, there are a sufficient number of fields that are essential and necessary to perform a classification with high accuracy, but there are also a large number of fields whose influence is difficult to assess at this stage. It should be emphasized that, on the one hand, an increase in the number of fields (features) for classification allows to increase the accuracy of classification, on the other hand, an increase in the number of features increases its complexity, therefore, after determining the best classification algorithms, it will be necessary to optimize the features of classification to form a minimally sufficient set of fields (features), which will ensure the specified classification accuracy.

Various metrics [3] will be used to evaluate the effectiveness of machine learning algorithms: accuracy, precision, recall, and F1 metric.

Accuracy means the ratio of correctly classified samples (packets) of the traffic flow to the total number of samples:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN}, \quad (1)$$

Precision is a measure of the ratio of positive, correctly predicted packets in traffic to the total number of positive classification predictions:

$$Precision = \frac{TP}{TP+FP}. \quad (2)$$

Recall measures the ratio of actual positive, correctly predicted packets in traffic:

$$Recall = \frac{TP}{TP+FN}. \quad (3)$$

The F1 metric represents the average of clarity and recall:

$$F1 = \frac{2 \cdot Precision \cdot Recall}{Precision+Recall}. \quad (4)$$

At the first stage of research, a list of applications that could not be successfully classified based on the data of the studied dataset was filtered. The

number of available packets was used as a filtering criteria. The 25 applications with the fewest packets (fewer than 500 packets in the dataset) were discarded.

Using a balanced dataset for the artificial neural network (ANN) algorithm, an assessment of the maximum achievable accuracy and its dependence on the speed code was performed.

Also, for the balanced dataset, an assessment of the best model parameters and classification accuracy was performed in the case of using the "random forest" (RF) algorithm.

The classification accuracy in this case depends on which packet fields (traffic information) are present in the dataset and on the importance of these fields for recognition. Therefore, in order to compare the importance of the fields, we conducted a study where we removed fields from the dataset that did not affect the accuracy of the classification (Fig. 1).

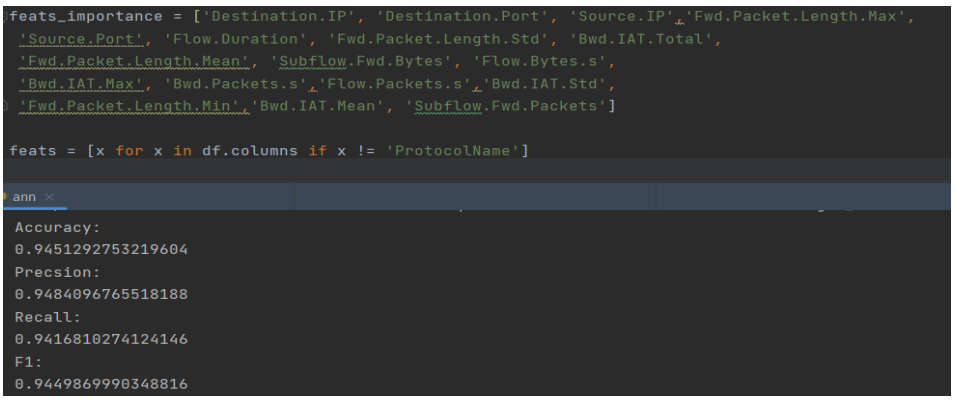


Fig. 1. Important of dataset fields for classification, which affect accuracy.

Conclusion. The scientific novelty consists in determining the parameters of machine learning algorithms that are optimal according to the criterion of accuracy for solving the problem of traffic classification in mobile communication networks of the 5th and 6th generations. Also, importance of the parameters (fields) of the dataset for classification are defined. The number of used field was decreased from 54 to 18 with decrease accuracy on 0.02. The proposed algorithms and parameters are the first stage of multi-step processing of packets in the network, which, together with clustering, slicing and distributed processing, will improve the efficiency of the mobile communication system in general.

References

1. Zaborovsky, V.S. (2010), Traffic analysis in packet switching networks, St. Petersburg: SPbGPU, 90p.
2. Bujlow, T., Carela-Español, V., Barlet-Ros, P. (2015), "Independent comparison of popular DPI tools for traffic classification", Computer Networks, No. 76, P.75-89. DOI: https://doi.org/10.1016/j.comnet.2014.11.001
3. AlZoman, R.M.; Alenazi, M.J.F. (2020), “A Comparative Study of Traffic Classification Techniques for Smart City Networks”, Sensors, No. 21, 4677, P. 1-17. DOI: https://doi.org/10.3390/s21144677

УДК 621.396

ОРГАНІЗАЦІЯ УПРАВЛІННЯ НАВКОЛОМІСЯЧНИМ УГРУПОВАННЯМ КУБСАТ (CUBESAT) ЗА ДОПОМОГОЮ МІСЯЧНОГО ПОСАДКОВОГО МОДУЛЯ

[1]Вигівський М.С., [1]Денисенко М.С., [1]Наритник Т.М., [2]Капштик С.В.
[1]*Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна*
[2]*Національний центр управління та випробувань космічних засобів*
E-mail: huaweibgablek@gmail.com; maxdeniss56@gmail.com; director@mitris.com; sergii.kapshtyk@gmail.com

ORGANIZATION OF CUBESAT CUBESAT MANAGEMENT WITH THE HELP OF THE LUNAR LANDING MODULE

In this work was discussesed proposals for organizing and managing the exploration and detection of valuable resources, as well as detailed study of the geology and composition of the Moon using a group of CubeSat optical-type satellites. It is proposed to place two landing modules on the poles of the Moon, each containing five CubeSat satellites. These satellites will use optical imaging to explore the surface of the Moon and search for valuable resources. The results obtained can be an important step in further space exploration and the exploration of the Moon.

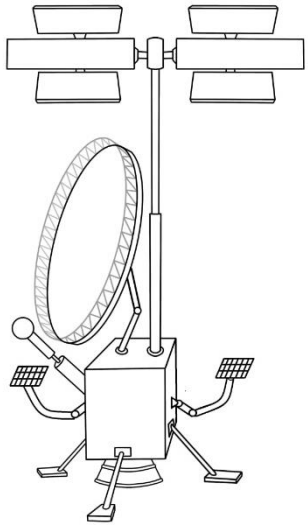
Місяць – єдиний природний супутник Землі. Тому через відносно невелику відстань, в масштабі галактики, він є потенційним об’єктом для колонізації, видобутку корисних копалин, створення місячної бази та космодрому, що буде виконувати функцію проміжної ланки (своєрідного транзитного пункту) між Землею й іншими, відносно близькими до неї, потенційними об’єктами колонізації. Отримані знання та відпрацьовані технології планується використати для подальшого освоєння космосу. Розуміючи важливість дослідження Місяця, США, Китай, Європа, Індія та інші країни розробляють власні та спільні Місячні місії для ретельного дослідження рельєфу, складу реголіту і місць скупчення та розподілу корисних копалин. Серед Місячних місій варто виділити Artemis: ця місія, яку планує запустити NASA, має на меті посадку першої жінки та наступного чоловіка на Місяць до 2024 року. Головна мета місії - дослідження для розбудови на Місяці постійної бази та розширення знань про поведінку людини в умовах низької гравітації. SMART-1: Ця місія була запущена Європейським космічним агентством (ESA) в 2003 році. Це була перша місія ESA на Місяць. Головною метою місії було дослідження Місяця та технологій польотів до інших планет. Місія використовувала іонний двигун для польоту до Місяця та проведення досліджень на його орбіті. Kaguya: Ця місія була запущена Японським космічним агентством (JAXA) в 2007 році. Метою місії було дослідження геології, магнітного поля та гравітації Місяця, а також пошук води та дослідження екології місячного оточення. Кагуя складалась з орбітального і місячного модулів, які виконували дослідження на орбіті та поверхні Місяця відповідно. Chang'e-3: Ця місія була запущена Китайською Національною Космічною Адміністрацією в 2013 році. Це була перша місія в світі, яка успішно виконала м'яку посадку на Місяць з китайським ровером "Yutu" (Західний заєць). Метою місії було дослідження геології та складу Місяця, а також випробування технологій для майбутніх місій з пілотами. Chandrayaan-2: ця місія була запущена Індійською Космічною Агенцією в 2019 році. Це була друга місія Індії на Місяць після Chandrayaan-1, яка відбулась в 2008 році. Метою місії було проведення досліджень Місяця з точки зору його геології, складу та розподілу води на поверхні та в глибинах. Місія також включала модуль для м'якої посадки та ровера, які мали провести дослідження на поверхні Місяця. Chang'e-5: ця місія, запущена

Китайською Національною Космічною Адміністрацією в 2020 році, мала на меті збір зразків Місячного ґрунту та його повернення на Землю для подальшого дослідження. Місія проводила дослідження Місяця з точки зору його складу та розподілу корисних ресурсів, таких як гелій-3 та титан.

Місяць пропонує багатство ресурсів, які можуть підживлювати навколоземну і місячну промислову інфраструктуру. Серед них можна виділити: сонячна енергія, ядерна енергетика, місячний реголіт, вода, водень, алюміній, кальцій, титан, гелій-3, платина, вуглець, азот, кремній, хром, залізо, магній, натрій, кисень та калій. Дослідження в рамках Експерименту зі складу місячної атмосфери (LACE) Аполлона-17 показують, що місячна екзосфера містить слідові кількості водню (H_2), гелію (He), аргону (Ar) і, можливо, аміаку (NH_3), вуглекислого газу (CO_2) і метан (CH_4). Велика кількість цих ресурсів є стратегічно важлива в космонавтиці та ракетобудуванні, а деякі стануть оновою для створення постійної місячної інфраструктури.

Оптична зйомка є одним з найбільш поширених методів для пошуку корисних копалин на Місяці. Це пов'язано з тим, що оптичні камери можуть знімати зображення поверхні Місяця з високою роздільною здатністю, що дозволяє детально вивчити геологію та склад місячної поверхні. Наприклад, на борту супутників Lunar Reconnaissance Orbiter (LRO) та Kaguya були встановлені оптичні камери, які здійснювали зйомку Місяця з високою роздільною здатністю. Крім того, місія Chang'e-5, запущена Китайською Національною Космічною Адміністрацією, використовувала оптичну камеру для визначення місць дослідження та взяття зразків. Оптична зйомка може допомогти виявити ознаки присутності корисних копалин, таких як метали, мінерали, гази та воду, на місячній поверхні. Зокрема, зміни у складі та кольорі поверхні Місяця можуть вказувати на наявність певних корисних копалин. Такі дані можуть допомогти в подальшому плануванні та проведенні місій на Місяць, включаючи видобуток та використання ресурсів.

Запропоновано створити систему дослідження Місяця, що складається із сегменту управління прийому та обробки корисної інформації і орбітального сегменту супутників CubeSat оптичного типу.

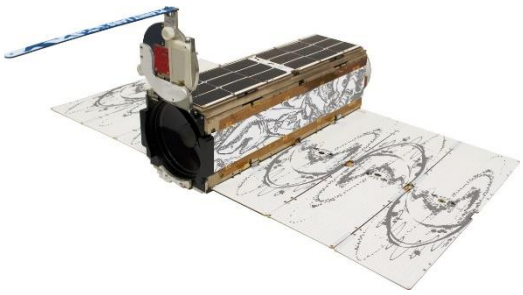


Супутники CubeSat необхідні для того, щоб робити знімки поверхні місяця в оптичному діапазоні. Вони можуть бути розташовані на круговій орбіті висотою 50 або 100 км від поверхні Місяця.

В якості прототипу може слугувати супутник Dove від компанії Planet Labs. Даний апарат може забезпечити роздільну здатність 38,9 см на орбіті висоті 50 км та 77,9 см на орбіті висоті 100 км.

Сегмент управління з двох посадкових модулів і п'яти супутників CubeSat на кожному із них, будуть запущені в одному комплексі. Це означає, що вони будуть знаходитися разом на борту ракети-носія. Прикріплення супутників CubeSat до посадкового модуля забезпечує їхню спільну мету - вийти на сонячну синхронну навколомісячну орбіту та початок руху в напрямку полюс-полюс навколо Місяця.

Коли комплекс буде доставлений на орбіту Місяця, посадковий модуль зі супутниками CubeSat буде відокремлений від ракети-носія. Після відокремлення, комплекс зробить кілька обертів по сонячній синхронній навколомісячній орбіті, щоб здійснити огляд поверхні Місяця та вибрати місце для посадки. Після вибору місця для посадки, посадкові модулі відділлять від себе апарати, що прикріплені до них, і сядуть в районі північного та південного полюса. Після посадки і того, як пил осяде, буде здійснене розгортання всього апарату. Також будуть розгорнуті спеціальні антени для забезпечення зв'язку із Землею та угрупованням супутників CubeSat. Ці процедури будуть допомагати забезпечити правильну роботу комплексу та забезпечити їх функціонування на Місяці.



Супутники CubeSat - це невеликі космічні апарати масою до 6 кг (5,8 кг), що будуть здійснювати картографування поверхні Місяця. Кожен супутник оснащений камерою з високою роздільною здатністю, яка може знімати зображення з висоти близько 50-100 км над поверхнею.

Однією з ключових переваг CubeSat є їх низька вартість.

Порівняно з більшими супутниками, виготовлення, запуск та експлуатація CubeSat є досить дешевими. Операційна система супутників може бути налаштована як на автоматичний так і на програмований збір даних. Кожен супутник відправляє зібрані дані на найближчий посадковий модуль, що знаходиться на полюсі, через передавач, який використовує X та S діапазони. Корисне навантаження на місячних супутниках CubeSat також може включати камери з високою роздільною здатністю, сенсори для вимірювання магнітного поля та радіації, а також пристрої для дослідження складу ґрунту та корисних копалин. За допомогою цих пристроїв можна досліджувати склад поверхні Місяця та досліджувати можливості використання його ресурсів для майбутніх місій на Місяці. До стандартного обладнання супутника Dove, пропонуємо додати ключовий інструмент для пошуку води, який називається рефлектометр з чотирма лазерами. Даний інструмент використала компанія Nasa для пошуку води на Місяці за допомогою місячного зонду Lunar Flashlight.

Нами пророблена тема проєкту який передбачає розташування на полюсах Місяця двох посадкових модулів [1]. Автономний модуль обладнаний приймально-передавальною офсетною антеною великого діаметру (8 м, 16 м або 24 м), яка забезпечує зв’язок в частотних діапазонах L та S. На сьогодні добре відпрацьована технологія проектування та виготовлення антен великого розміру, які використовуються у складі геостаціонарних супутників типу Inmarsat-4, Inmarsat-6, Thuraya [2]. Опромінювач антени встановлений на відкидну мачту і обладнаний механічним приводом для відстеження зміни місця розташування антени на поверхні Землі. Даний модуль забезпечує стабільне функціонування інфокомунікаційної системи Місяць-Земля. На посадкових модулях, які знаходяться на північному та південному полюсах Місяця, також встановлені антени, які забезпечують зв'язок зі супутниками CubeSat. Основною задачею штучного інтелекту на борту модуля буде обробка знімків, що отримані від супутників, та формування траєкторії на наступний виток. Використання глибинного навчання та нейронних мереж, дозволяє отримувати більш точні та деталізовані зображення поверхні супутника. Оскільки зв'язок з Місяця на Землю може бути затриманий через відстань, то штучний інтелект може бути використаний для обробки даних з супутників, щоб зменшити їх обсяг, а також забезпечити якіснішу передачу даних.

У запропонованому модулі передачі будуть використовуватись дві цифрові антенні решітки (ЦАР) з різними діапазонами, розташовані на протилежних сторонах оболонки модуля. Після приземлення решітки будуть притиснуті до корпусу за допомогою механічних кронштейнів та розкриються під кутом 90° відносно модуля. Кожна ЦАР має саморегульовану кріпильну конструкцію, що дозволяє регулювати кут нахилу по осях X та Y для стабільного прийому сигналу. Перша ЦАР буде працювати в L діапазоні на частоті 2.1 ГГц для прийому телеметричної інформації від супутників. Друга ЦАР буде працювати в діапазоні X на частоті 7-8 ГГц та призначена для передачі інформації на борт супутника для підтримки роботи штучного інтелекту, обробки та забезпечення необхідної інформації.

Таблиця 1. Кількість елементів в залежності від ширини ДН.

Ширина ДН (°)	2.1 ГГц	7-8 ГГц
5	6	7
3	10	11
1	29	31

Так як решітка буде квадратної форми, то в залежності від того яка буде ширина діаграми направленості (ДН) буде залежать кількість елементів в цій решітці. Таблиця 1 містить розрахунки кількості елементів в залежності від ширини ДН для двох діапазонів S та X при відстані між елементами, рівній половині довжини хвилі.

Таблиця.2. Результати розрахунку тривалості сеансу зв'язку.

Показник	h = 50 км		h = 100 км	
Роздільна здатність супутника CubeSat	38.9 см		77.9 см	
Перша космічна швидкість	1.6795095 км/с		1.67948534425 км/с	
Орбітальний період (T)	6782.251 с		7068.818 с	
Кут місця супутника (β)	+10°	+15°	+10°	+15°
Кут між початком і закінченням сеансу зв'язку (2φ)	6.775°	5.12°	11.347°	9.017°
Тривалість сеансу зв'язку	255.276 с	192.917 с	445.61 с	354.109 с

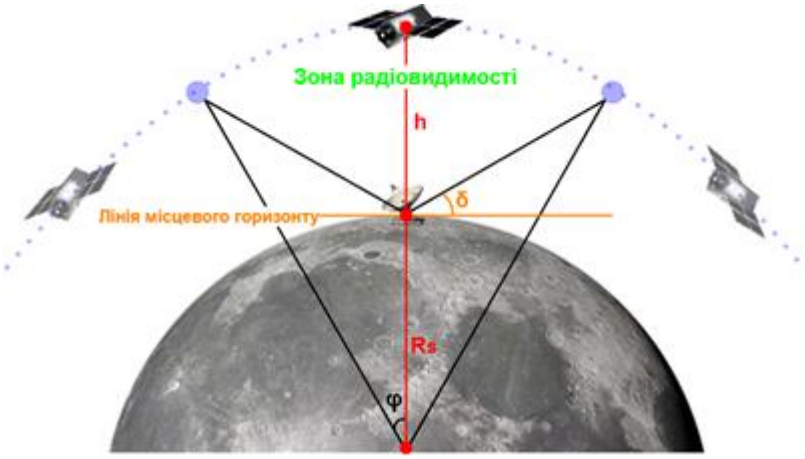


Рис. 1. Розрахунок тривалості сеансу зв'язку.

Висновки.

1. Дослідження поверхні Місяця є однією з найбільш актуальних тем в космічній галузі, оскільки це може допомогти в розвитку наукових знань про космос та покращенні космічних технологій. Для здійснення такого дослідження запропоновано використовувати космічні апарати типу CubeSat, які є невеликими та компактними. Використання таких апаратів дозволяє знизити витрати та ризики, пов'язані зі здійсненням космічних місій, та відкриває нові можливості для наукових досліджень.

2. В цій роботі для ефективного та оперативного управління космічними апаратами типу CubeSat запропоновано використовувати керування з поверхні Місяця. Такий підхід дозволить зменшити затримки при передачі сигналів, що виникають через велику відстань між космічним апаратом та Землею.

3. Запропоновано розмістити на поверхні Місяця посадковий модуль, який буде мати високотехнологічне обладнання для управління та забезпечення стабільної роботи інфокомунікаційної системи Місяць-Земля. Цей модуль забезпечить необхідний рівень зв'язку та передачі даних між Землею та Місяцем, що буде корисним для проведення наукових досліджень та діяльності у галузі космічних технологій..

4. Запропоновано конструктивно-компонувальне рішення для даного модуля яке дає зрозуміти де можна розташувати цифрові антенні решітки.

Література

1. Ільченко, М. Ю. ., Вигівський, М. С. ., Наритник, Т. М. ., & Капштик, С. В. . (2022). ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА ДЛЯ ІНФОРМАЦІЙНОЇ ПІДТРИМКИ МІСІЙ З ВИВЧЕННЯ ТА ОСВОЄННЯ МІСЯЦЯ. Збірник матеріалів Міжнародної науково-технічної конференції «ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ», 34–38. вилучено із http://conferenc.its.kpi.ua/proc/article/view/255174
2. Inmarsat-6 F1, 2 (GX 6A, 6B) / Електронний ресурс. Режим доступу: https://space.skyrocket.de/doc_sdat/inmarsat-6.htm

УДК 004.75

МІКРОСЕРВІСНА АРХІТЕКТУРА ТА ЇЇ ЗАДАЧІ НА ПРИКЛАДАХ З РЕАЛЬНОГО ЖИТТЯ

Дмитренко О.А.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: olexandra.dmytrenko@gmail.com

MICROSERVICE ARCHITECTURE AND ITS TASKS ON EXAMPLES FROM THE REAL LIFE

Distributed systems and microservice architecture require in-depth understanding so that consensus problems do not arise during the process of approbation of the system but are solved at the stage of planning and technology selection. This article provides a description and comprehensible general comparison of microservice architecture with real-life problems. The "Two Generals' Problem" and "Byzantine Fault" issues with the possible solutions are described in the article. The presentation of the Paxus algorithm and ideas that go around it are also presented.

Розподілені системи та мікросервісна архітектура потребують досконального розуміння, аби задачі консенсусу не виникали в процесі апробації системи, але вирішувались на етапі планування та вибору технологій. У даній статті наведено опис та зрозумілі широкому загалу порівняння мікросервісної архітектури з задачами реального життя, та розглянуто задачі «двох генералів», «візантійських генералів». В тексті також описано можливі вирішення цих проблем, в тому числі, наведена ідея Паксус алгоритму.

Людський мозок - це загадка. Людина може дійти у своїх роздумах та уявленнях до того, що ніколи не існувало. Розум нам допомагає створювати нове та небувале, але в той же час, речі, які ми намагаємось створити, творяться за образом та подобою того, що вже існує. Наприклад, винаходячи літак, людина дивилась на птаха, роботи створюються щоб повторювати тіло людини та бути на нас схожими, машинний інтелект та нейронні мережі – щоб бути пародією на мозок людини та скомбінувати надможливості мозку у вигляді комп'ютерів із емоційною складовою, яка братиметься з даних про прийняття рішень реальних людей. У даній статті я описую мікросервісну архітектуру та ключові задачі консенсусу у вигляді порівнянь з усім відомими об'єктами та життєвими ситуаціями, щоб полегшити розуміння на перший погляд складних речей.

Мікросервісна архітектура – це багатоетапне виробництво. Зараз поширення набрала мікросервісна технологія, яка має під собою розподілену систему, або ж систему, що поділена на функціональні частини, які, зазвичай, можуть реплікуватись у випадку великого навантаження на них з метою ефективного реагування на кількість запитів, що необхідно обробляти. Раніше, натомість, застосунки розроблялись як моноліти, які обробляти стільки запитів, скільки обробляло їх найвужче місце. Також існує проміжний варіант — множення одного монолітного сервісу на декілька додаткових серверів. Іншими словами, повноцінне програмне забезпечення існуватиме в декількох репліках. При організації рівномірного розподілення навантаження, це дозволить підвищити відмовостійкість застосунку, і, таким чином, пропускна можливість підвищиться. Мінусом даного підходу є менш ефективне використання ресурсів ніж у випадку мікросервісної архітектури, де, за потреби, збільшується тільки кількість необхідних елементів системи, а не створюється додаткова повноцінна система.

В сучасному світі, незабаром після того, як людство освоїло певну технологію, з'являються покращені версії цієї технології, або відбувається адаптація ідеї в інші сфери

вжитку. Цікавим є те, що все нове насправді є старим і далеко не завжди забутим, те саме вже десь існувало, але в інших іпостасях, інші, і не обов'язково вчені, ці ж проблеми вже вирішував, тільки не завжди у тому самому середовищі.

Кажучи про винайдення мікросервісної архітектури, її ідею можна порівняти зі звичайним виробництвом, наприклад, сирним. В залежності від етапу виробництва, потрібна різна кількість ємностей та місця для пастеризації молока, відстоювання його після скисання та витримки сиру. Моноліт можна проасоціювати, з виробництвом, що має місце в одному приміщенні, де підтримується різна температура в залежності від етапу. Якщо етап витримки сиру займає багато часу, то виробництво чекатиме, доки даний етап не закінчиться.

Мікросервісною архітектурою було б створення різних кімнат, можливо, навіть, приміщень, для відповідних процесів з необхідною для них температурою та кількістю ємностей. Тоді б можна було в режимі реального часу приймати нове молоко та починати його обробляти. У випадку збільшення поголів'я корів, можна було б додатково розмістити більшу кількість ємностей в одні кімнати, а якщо розміри не дозволяються, побудувати нові зали, призначені для певного процесу. Відзначу, що зважаючи на об'єми різного роду сировини, додаткові приміщення можуть знадобитись для скисання молока, адже пастеризація проходить швидше, ніж скисання, та існуючих потужностей може вистачити. Сир не займає багато місця, а отже і для його зціджування можливо вийде обійтись лише додатковими стелажами. Якщо кількість вхідного молока зменшуватиметься, додаткові кімнати та ємності можна не заповнювати сировиною, а отже і не витрачати додаткові кошти на підтримку робочого стану. Словами мікросервісної архітектури, ми збільшуємо чи зменшуємо кількість робочих серверів, виділених на певний мікросервіс, або ж залучаємо додаткові потоки для обробки вхідних запитів.

Задача гарантованої комунікації або двох генералів. Добре, коли новий процес працює, полегшує життя та робить його якіснішим. Але ж зазвичай, з ускладненням самого виробництва, необхідно створювати нові та додаткові процеси. Наприклад, розташувавши різні частини виробництва в різних приміщеннях, необхідно організувати транспорт між приміщеннями, що вимагатиме не тільки додаткових вкладень, але і ставитиме під загрозу саме виробництво, у випадку неможливості транспортування через відсутність бензину, електрики, поламки транспортних засобів, сторонніх подій, що заважатимуть руху, тощо. Проводячи аналогію з мікросервісною архітектурою, потрібно організувати відправлення повідомлень між частинами застосування. Це, в свою чергу, створює питання доставки сповіщень, а також їх правдивість.

Проблема транспортування сповіщень між елементами розподіленої системи опублікована ще у 1975р у [0] та отримала назву «Задача двох генералів» у 1978р. Суть полягає в тому, що два генерали атакують спільного ворога, армія якого розташована між арміями спільників. Успіх буде тільки у випадку одночасної атаки, про яку слід домовитись. Головний генерал має надіслати іншому сповіщення про атаку, а також отримати від нього підтвердження. Далі можливі дві негативні ситуації: до другого генерала не доїде гінець, або ж сповіщення буде отримано, але перший генерал не отримає підтвердження через перехоплення гінця на зворотному шляху. Таким чином, неможливо гарантувати, що обидві армії підуть в атаку на ворога в один і той самий час.

Вище наведено рисунпк 1 з [0], що описує наведену проблему мовою мікросервісної архітектури. P1 (partition 1) та P2 (partition 2) – це окремі мікросервіси, між якими має відбутись комунікація. IPCM – inter process communication mechanism, тобто механізм кожної сторони, через який відбувається комунікація, наприклад, REST протокол. Network – мережа, яка з одного боку служить шляхом комунікування, а з іншого, – може порватись в любий момент, тому асоціюється з ворожою армією.

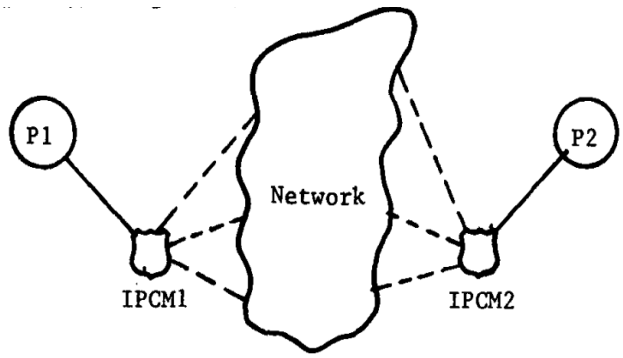


Рис. 1. Задача двох генералів у розподіленій мережі.

Задача гарантування отримання відповіді відправником не має розв'язку. Тим не менш, ситуація достатньо поширена тому нижче я наводжу способи суттєво зменшити вірогідність неотримання відповіді.

1) Побудувати безпечний канал зв'язку між двома арміями, але це додаткові ресурси.

2) Замість надсилання одного гінця надіслати багато, наприклад, 100. Інформацію вважати прийнятою у випадку отримання однієї чи декількох відповідей. Декілька відповідей може знадобитись коли сповіщення може бути підроблене по дорозі.

3) Заради оптимізації ресурсів, можна відправляти кожного наступного гінця після того, як пройшов час, за який мав повернутись перший.

Додатково, щоб зрозуміти якість каналу, можна нумерувати сповіщення та робити висновки з отриманих результатів.

Задача неправдивих сповіщень або візантійських генералів. Окрім питання доставлення сповіщень, постає питання правдивості отриманих сповіщень. Якщо зв'язок погано захищений, то по дорозі можна підробити сповіщення. Тим не менш, така проблема може статись навіть при захищеному з'єднанні, коли в одного мікросервіса чи розподіленої бази даних з різних причин застаріла інформація, яка вже неактуальна. Тобто, необхідно гарантувати, що або ж інформація буде останньою, або даний вузол системи не братиме учать в консенсусному прийнятті рішення.

Проводячи паралель з реальним життям – можемо уявити армію, що складається з багатьох легіонів. Головний генерал, який може бути зрадником, має дати наказ генералам легіонів або нападати або відступати. Зважаючи на те, що субординати можуть теж бути зрадниками, і їх може бути до третини, успіх буде тільки у випадку нападу всіма чесними генералами. Таким чином, накази головнокомандуючого слід перевіряти, а без комунікації війна буде програною. Дана задача називається «Задачею візантійських генералів» і також не має розв'язку. Така проблематика була описана у 1985 році у [0] та ставила під питання невалідність тільки одного вузла системи. Тим не менш, схожу задачу розглядали ще з 1950х років у NASA та у авіаційній галузі з метою створення бортових комп'ютерів, які б мали

- декілька реплікацій даних та окремих обчислювальних машин, а також,
- паралельні процеси однакових обчислень, які б гарантували правильність висновків та максимально унеможливлювали помилку,
- шукали та знаходили помилку методом порівняння результатів та голосуванням (більшість однакових результатів вказує, що це правильний результат)
- виправляли помилку,
- реконфігурувались щоб позбавитись зламаних вузлів та не брати їх «думку» до уваги [0].

У наведеній статті [0] використовувалось шість реплікацій для забезпечення коректної роботи тогочасних літаків, які обмінюються станом між собою кожні 50мс, але в загальному випадку реплікацій може й не потрібно стільки. Наприклад, в Європе́йській організації з я́дерних досліджень, що знаходиться в Женеві, використовується три репліки даних, які розташовані в трьох різних країнах на випадок війни та бомбардувань. Варто зазначити, що кількість даних величезна, адже йдуть записи щомоментного розташування частинок в адронному колайдері.

Паксос протокол та модель частково працюючого парламенту. Існує не один алгоритм, що допомагає вирішенню проблеми візантійських генералів. Я хочу навести алгоритм, який вирішуючи проблему нерегулярності роботи окремих вузлів, також, вирішував проблему оповіщення новими законами депутатів, які час від часу виходили з зали засідань. Стаття, що описує даний алгоритм була надрукована у 1989 Леслі Лампортом, але до неї поставились серйозно пізніше, коли була надрукована стаття без порівняння процесу з грецьким парламентом на острові Паксос.

Ідея алгоритму полягає у тому, що за допомогою порівняння поточного стану системи та метаінформації про дані на етапі їх зчитування з різних реплік, шляхом голосування приймається рішення, які саме дані валідні, якщо вони не співпадають.

Нижче я опишу реалізацію запису та читання інформації за Паксос алгоритмом.

Існує три ролі:

Пропонувач – пропонує закони або ж висловлює бажання запису певної інформації, нумеруючи її у зростаючій послідовності.

Приймачі – депутати, які розглядають нові закони, або ж вузли системи, які отримують сповіщення. Розгляд відбувається тільки у випадку, якщо є кворум (більшість працюючих вузлів системи).

Секретар (учень) – який, бере-запиує виключно прийняті закони, та віддає їх кінцевому користувачу [0].

Метод, через який відбувається голосування заснований на порівнянні максимального номеру вже існуючого запису в пам’яті вузла. Тобто, якщо новий номер більший за вже існуючий, приймач відповідає обіцянкою не розглядати сповіщення з меншим номером, а якщо ні – приймач відхиляє запис та у відповідь надсилає максимальний наявний в нього номер. Якщо більшість приймачів відповіла обіцянками прийняти сповіщення, воно буде розіслане з запитом «прийняти» усім наявним вузлам, і вони мають його прийняти, якщо попередньо не відповіли, що мають вищий номер. Сповіщення відсилається клієнтам тільки після того, як воно було прийняте кворумом [0].

Висновки. З кожним днем кількість розподілених систем стає все більше й більше, адже бізнесмени хочуть бути впевненими, що їх продукт витримає любе навантаження та залишиться працювати навіть у випадку бомбардувань в місці з частиною серверів. Питання вирішення конфліктних ситуацій у розподілених системах залишається актуальним вже 70 років, адже з розвитком інформаційних технологій з’являються нові нюанси, ідеї та потреби. Зважаючи на те, що навчання нового покоління, а також розвиток професіоналів потребують вигадливості та простоти, аби бути почутим та зрозумілим, я навела деякі сучасні задачі та побудови розподілених систем, які походять ще з давнини, та запропонувала їх розв’язки.

Література

1. Akkoyunlu, Eralp A., K. Ekanandham and Richard Huber. “Some constraints and tradeoffs in the design of network communications.” // presented at the Proceedings of the fifth ACM symposium on Operating systems principles, SOSP '75, 1975, 01 листопада, ст. 67-74, DOI:10.1145/800213.806523
2. Michael J. Fischer, Nancy A. Lynch, and Michael S. Paterson. Impossibility of distributed consensus with one faulty process. J. ACM 32, Volume 32, Issue 2, 1985 квітень, 374–382, DOI:10.1145/3149.214121
3. Goldberg, Jack. “The SIFT computer and its development.”. Digital Avionics Systems Conference, 1981. ст.285-289 DOI:10.2514/6.1981-2278.
4. Kevin Babitz. “The Strange Story of the Paxos Algorithm”. 2021, 18 лютого. [Онлайн] https://towardsdatascience.com/the-strange-story-of-the-paxos-algorithm-52a9f3f53ae0
5. Leslie Lamport. 1998. The part-time parliament. ACM Trans. Comput. Syst. 16, 2 (May 1998), 133–169, DOI:10.1145/279227.279229.

УДК 621.395

МЕТОД ПОБУДОВИ ЗАВАДОСТІЙКОГО ПРОГРАМНОГО КОМПЛЕКСУ З ВИКОРИСТАННЯМ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ

Маньківський В.Б., Омельченко С. А.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: v.b.mankivskiy@gmail.com , llamemnonal@gmail.com

THE METHOD OF BUILDING A FAULT-TOLERANT MICROSERVICE SOFTWARE COMPLEX

This article describes the principle of operation and construction of a software system using microservice architecture, as well as the risks and benefits. Comparison of monolithic and microservice architecture. The algorithm for obtaining a noise-resistant software system for uninterrupted operation of the service is described.

У роботі описано принцип роботи та побудову програмного комплексу з використанням мікросервісної архітектури, вказані ризики та переваги. Порівняно монолітну та мікросервісну архітектуру. Описано алгоритм отримання завадостійкого програмного комплексу для безперебійної роботи сервісу.

Архітектура мікросервісів переносить логіку додатків у сервіси та використовує мережевий рівень для зв'язку між ними. Спілкування в мережі замість викликів у пам'яті призводить до додаткової затримки та складності системи, що вимагає взаємодії між кількома фізичними та логічними компонентами. Підвищена складність розподіленої системи призводить до більш високої ймовірності відмови окремих мереж. В цьому полягає основний ризик мікросервісної архітектури. При розробці мікрослужби завжди корисно подумати про те, як вона поводитиметься, якщо певний компонент не працює. Це допоможе створити відмовостійкий сервіс. Відмовостійкість (англ. "fault tolerance") це властивість, що дає змогу системі продовжувати нормально працювати в разі виходу з ладу деяких її компонентів.

Необхідно переконатися, що послуги не сильно залежать від одного компонента. І якщо вони виявляться залежними необхідно розробити стратегію швидкого відновлення після збою. В цьому і полягає різниця між монолітною архітектурою та мікросервісною архітектурою, у підходах до розбиття програмного забезпечення на компоненти та їх взаємодії. Адже у монолітній архітектурі весь програмний код та функціональні модулі розміщені в одному монолітному додатку. У цій архітектурі всі компоненти додатку взаємодіють між собою напряму, тому виникає проблема залежності компонентів один від одного. Це може призводити до складнощів з масштабуванням, розширенням додатку, а також зі збільшенням складності управління додатком та ризику виникнення помилок. Тому для побудови завадостійкого програмного комплексу краще використовувати мікросервісну архітектуру.

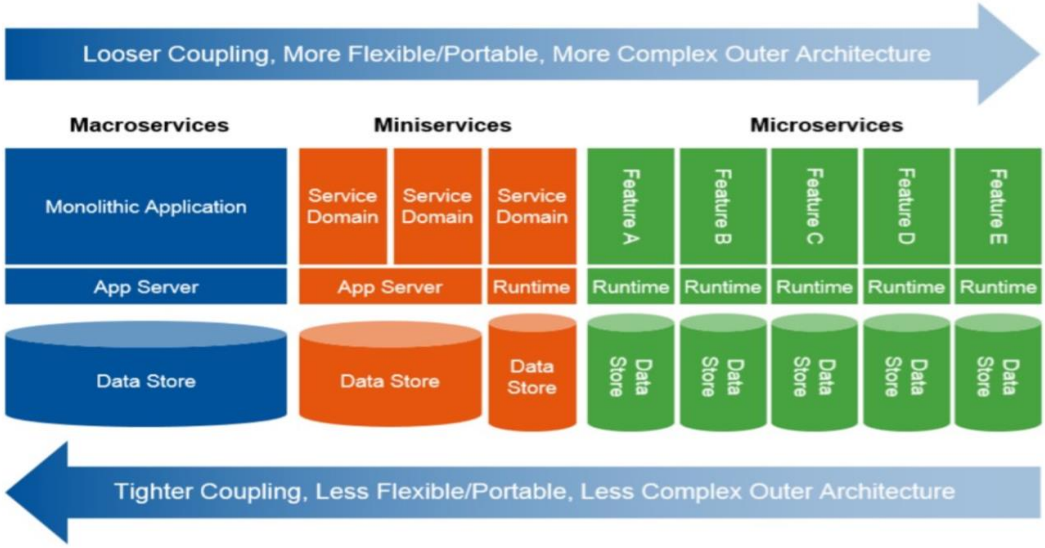


Рис. 1. Приклад сервісних архітектур.

Один із сучасних підходів у розробці інформаційних систем передбачає використання систем контейнеризації додатків для створення ізольованого оточення.

Першим плюсом цього підходу є незалежність оточення кожного додатка від встановлених на ЕОМ, що виконує контейнери, програм, що забезпечує прозорість і передбачуваність роботи додатка та захищає від перетину залежностей різних версій.

Другим плюсом є наявність механізмів управління та відстеження життєвого циклу контейнерів. Сучасні системи управління контейнерами (Docker Swarm, OpenShift , Kubernetes, Nomad) дають змогу контролювати стан програми всередині контейнера через настроюваний механізм перевірок і перезапускати неробочі контейнери.

Третім плюсом є декларативна система конфігурування розгортання програми. Під час розгортання потрібно вказати нову конфігурацію, і оркестратор приведе систему до потрібного стану, що дає змогу уникнути помилок під час імперативного написання команд. Важливим плюсом є можливість запускати оркестратор контейнерів на декількох ЕОМ, з'єднаних спільною мережею. Використання оркестратора в режимі декількох вузлів забезпечує безперебійну роботу контейнерів і їх переміщення на вільні вузли в разі відмови одного з них.

Окрім переваг, необхідно пам’ятати і про недоліки. Основний недолік мікросервісної архітектури – це продуктивність, скільки процеси проходять між сервісами, а от же в загальний час доданий час мережевої затримки між сервісами.

На відміну від монолітної архітектури (макросервісної), де лінії зв’язку – це внутрішня шина сервера. Це є основним обмеженням мікросервісної архітектури, яке потрібно розглядати, як особливість її і проектувати рішення виходячи з нього.

Отже, для побудови завадостійкого програмного комплексу з використанням мікросервісної архітектури необхідно виконати наступні кроки:

1. Аналіз вимог до системи та її функціональності.

2. Розробка незалежних мікросервісів: кожен мікросервіс повинен виконувати конкретну функцію, відповідальну за один або декілька зв'язаних між собою бізнес-процесів. Кожен мікросервіс повинен мати власну базу даних та інші ресурси, які не використовуються іншими мікросервісами.

3. Застосування контейнерів: Контейнери дозволяють ізолювати різні частини програмного комплексу, що сприяє зменшенню взаємодії між компонентами і забезпечує більшу стійкість системи до відмов.

4. Розробка API для мікросервісів: для взаємодії між мікросервісами необхідно розробити API, яке буде використовуватися для передачі даних та комунікації між мікросервісами.

5. Розробка механізмів відновлення: для забезпечення завадостійкості системи необхідно розробити механізми відновлення, які забезпечують автоматичне відновлення роботи системи в разі збоїв або помилок. Наприклад, механізми відновлення можуть включати автоматичне перенаправлення запитів до резервних мікросервісів, автоматичне відновлення бази даних або автоматичну перезавантаження мікросервісів.

6. Тестування та моніторинг: для забезпечення завадостійкості системи. Впровадження механізмів тестування та автоматизації розгортання та масштабування мікросервісів та встановлення системи моніторингу та контролю за роботою кожного мікросервісу і всього програмного комплексу в цілому. Це дозволить оперативно виявляти та вирішувати проблеми в системі.

Література

1. Gigi Sayfan. Hands-On Microservices with Kubernetes. Packt Publishing, 1st edition 2019, - p.p. 58-90.
2. Stephen Fleming. Microservices Architecture Handbook: Non-Programmer's Guide for Building Microservices. CreateSpace Independent Publishing Platform 2018, - p.p. 62-73.
3. P.S. Kocher. Docker microservices and containers, Addison-Wesley Professional, 1st edition 2019, - p.p. 189 -201.
4. Orkhan Gasimov. Microservice architecture for beginners. https://www.globallogic.com/ua/insights/blogs/microservices-architecture-for-beginners-part-one/
5. Newman S. Creating microservices, 2016, - p.p. 124-149.
6. M. Fowler. Enterprise software application architecture, Addison-Wesley Professional, 1st edition 2006, p. 544.
7. Neal Ford. Building Microservice Architectures, 2015, p. 20.

УДК 004.6

ОПТИМІЗАЦІЯ ВИКОНАННЯ ЗАПИТІВ У РЕЛЯЦІЙНІЙ СИСТЕМІ УПРАВЛІННЯ БАЗАМИ ДАНИХ

Єрмолаєв О. Д., Суліма С.В.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: itssulima@gmail.com

OPTIMIZATION OF QUERIES EXECUTION IN THE RELATIONAL DATABASE MANAGEMENT SYSTEM

A method of optimizing the synthesis of complex SQL queries from many simple ones is presented, which allows to increase the speed of execution of the input query by the relational database while simultaneously ensuring high performance and ease of use.

Обробка SQL – це синтаксичний розбір, оптимізація, генерація джерела рядків та виконання оператора SQL. На рис. 1 зображені загальні етапи обробки SQL запиту.

Рис.1. Загальні етапи обробки SQL запиту.

Щоб допомогти програмістам баз даних, на ринку існує безліч інструментів автоматизації налаштування SQL, які допомагають виявляти проблемні SQL-оператори та пропонують варіанти їх виправлення [1]. Незважаючи на те, що автоматичні інструменти можуть полегшити налаштування SQL, воно все одно потребує значної участі людини.

Щоб забезпечити оптимальну продуктивність складання набору запитів, рекомендується використовувати метод проб і помилок, тобто написати кілька варіантів запитів та порівняти їх плани планування та виконання. Дослідники запропонували багато різних методів та порад, які можна використовувати для підготовки та тестування оптимізації продуктивності запитів [1-6]. Найбільш поширеними методами визначення найкращих можливостей складання запитів є аналіз кількості логічних даних, створених запитів та перегляд графічних планів.

Тимчасові таблиці – функція, яка дозволяє зберігати та обробляти проміжні результати за допомогою тих самих можливостей вибору, оновлення та приєднання, які можна використовувати з типовими таблицями SQL Server [7]. Тимчасові таблиці мають різні варіанти, включаючи, серед іншого, локальні тимчасові таблиці (починаються з #), глобальні тимчасові таблиці (починаються з ##) та змінні таблиці (починаються з (@). Збережені процедури можуть посилатися на тимчасові таблиці, створені під час поточного сеансу.

Отже, удосконалений метод, який пропонується далі, засновується на уникненні оператора IN в реченні WHERE [8].

Рішення:

Створити тимчасову таблицю і вставити необхідні дані і ПРИЄДНАТИСЬ до основного запиту.

Якщо складний запит включає оператор IN, його необхідно видалити, а для створення тимчасової таблиці і включення її в запит необхідно виконати наступні кроки:

1. Визначте поля SELECT замість SELECT *: Якщо таблиця має багато полів і рядків, виділення всіх стовпців (за допомогою SELECT *) надмірно використовує ресурси бази даних для запиту великої кількості непотрібних даних. Визначення полів у операторі SELECT вкаже базу даних на запит лише необхідні дані.
2. Уникайте SELECT DISTINCT, якщо це можливо: SELECT DISTINCT працює, групуючи всі поля в запиті, щоб створити чіткі результати. Однак для досягнення цієї мети необхідна велика кількість обчислювальної потужності.
3. Використовуйте WHERE замість HAVING для визначення фільтрів: Відповідно до порядку операцій SQL, оператори HAVING обчислюються після операторів WHERE. Якщо нам потрібно відфільтрувати запит на основі умов, оператор WHERE є більш ефективним.
4. Використовуйте LIMIT для вибірки результатів запиту: Перед першим запуском запиту переконайтеся, що результати будуть бажаними та значущими, використовуючи оператор LIMIT. Слід зазначити, що в деяких

СУБД – LIMIT просто не існує, тому зручно використовувати даний синтаксис:

SELECT TOP 3 * FROM Table;

5. Замініть підзапит на JOIN: Хоча підзапити корисні, їх часто можна замінити об'єднанням, яке, безумовно, виконується швидше. Розглянемо приклад нижче:

```
SELECT a.id, (SELECT MAX(created)
FROM posts
WHERE author_id = a.id)
AS latest_post FROM authors a
```

Щоб уникнути підзапиту, його можна переписати за допомогою об'єднання як:

```
SELECT a.id, MAX(p.created) AS latest_post
FROM authors a
INNER JOIN posts p
ON (a.id = p.author_id)
GROUP BY a.id
```

6. Видалити оператор IN, створити таблицю #temp і вставити в неї необхідні дані.
7. Створити індекс для таблиці #temp.
8. З'єднайте #temp з базовою таблицею

Запропоновано удосконалений метод оптимізації SQL запитів у випадку якщо швидкість вибірки даних почала просідати за часом, який використовує заміну оператора IN на тимчасову таблицю та використовує не кластеризований індекс, що дозволяє на відміну від існуючих пришвидшити вибірку за рахунок зменшення логічних звернень.

Література

1. M. L. Rupley, "Introduction to query processing and optimization," Indiana University, South Bend, South Bend, IN, USA, techreport TR– 20080105–1, 2008.
2. R. Bhajipale, P. Bisen, A. Meshram, and S. S. Thakur, "SQL tuner," International Journal of Computer Trends and Technology, vol. 33, no. 1, pp. 29–32, 2016.
3. P. Karthik, G. T. Reddy, and E. K. Vanan, "Tuning the SQL query in order to reduce time consumption," International Journal of Computer Science Issues, vol. 9, no. 4/3, pp. 418–423, 2012.
4. J. Habimana, "Query optimization techniques – tips for writing efficient and faster SQL queries," International Journal of Scientific & Technology Research, vol. 4, no. 10, pp. 22–26, 2015.
5. R. Sahal, M. Nihad, M. H. Khafagy, and F. A. Omara, "iHOME: Index based JOIN query optimization for limited big data storage," Journal of Grid Computing, vol. 16, no. 2, pp. 345–380, 2018.
6. M. Sharma, "Query optimization using SQL transformations," International Journal of IT, Engineering and Applied Sciences Research, vol. 1, no. 1, pp. 100–104, 2012.
7. Phil Factor Тимчасові таблиці URL: https://www.red-gate.com /simple-talk/sql/t-sql programming/temporary-tables-in-sql-server/.
8. Єрмолаєв, О. Д. Метод оптимізації SQL запитів : дипломна робота … бакалавра : 172 Телекомунікації та радіотехніка / Єрмолаєв Олександр Дмитрович. – Київ, 2021. – 56 с.

УДК 621.391

КОМПЛЕКСНИЙ МЕТОД ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ОБРОБКИ НАВАНТАЖЕННЯ У РОЗПОДІЛЕНИХ ЦОД ОПЕРАТОРІВ ЗВ'ЯЗКУ

Глоба Л.С., Райчук А.А., Прокопець Н.А.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: raaukr@gmail.com

A COMPLEX METHOD OF INCREASING THE EFFICIENCY OF LOAD PROCESSING IN DISTRIBUTED DATA CENTERS OF COMMUNICATION OPERATORS

The article proposes a solution to the problem of preventing a rapid increase in electricity consumption in remote data centers by increasing the energy efficiency and productivity of information and communication network (ICM) load maintenance while meeting the requirements for the availability of its maintenance system by applying a comprehensive method of energy-efficient load maintenance.

The demo aims to analyze the proposed comprehensive method, which allows us to claim that it meets the requirements for the availability of the service system and gives an efficiency gain of 15.722% compared to Backfill and 88.887% compared to Round Robin.

Розвиток сучасних інформаційно-комунікаційних технологій, зокрема технологій віртуалізації, зумовив появу тенденції програмної реалізації апаратних функцій, яка сприяла розвитку технологій і концепцій: NFV, SDN, Network Slicing, Edge Computing, bDDN. Ці технології вимагають значного обсягу обчислень, які виконуються у віддалених Дата Центрах (у Cloud середовищі) і, відповідно, споживають значну кількість енергії під час обробки навантаження. Функціонування інфраструктури територіально розподілених ЦОД є енерговитратним та вносить суттєвий вклад у загальне енергоспоживання сучасних інформаційно-комунікаційних мереж (ІКМ). У зв’язку з цим особливої актуальності набуває вирішення проблемних питань із забезпечення енергоефективності розподілених ЦОД. За даними досліджень [1, 2], частка споживання електроенергії такими системами станом на 2020 рік становила близько 1% усієї електроенергії, що виробляється у світі.

Згідно глобальної оцінки споживання енергії центрами обробки даних на 2030 рік загальне середнє енергоспоживання дата центрів у світі складатиме 848 TWh, а максимальне значення може скласти близько 1929 TWh [3].

Існує велика кількість підходів з підвищення енергоефективності роботи дата центрів, але вони не враховують одночасного забезпечення трьох основних показників: продуктивності, енергоефективності та дотримання вимог SLA.

У статті пропонується вирішення задачі запобігання стрімкому збільшенню споживання електроренергії у віддалених дата центрах за рахунок підвищення енергоефективності та продуктивності обслуговування навантаження інформаційно-комунікаційної мережі (ІКМ) при виконанні вимог щодо доступності системи його обслуговування за рахунок застосування комплексного методу енергоефективного обслуговування навантаження.

Демо націлено на аналіз запропонованого комплексного методу, який дозволяє стверджувати, що він забезпечує виконання вимог щодо доступності системи обслуговування та дає виграш за критерієм ефективності на 15,722% у порівнянні із Backfill та на 88,887% у порівнянні з Round Robin.

Огляд підходів щодо енергоефективного комп’ютінгу. Згідно з рекомендаціями Міжнародного союзу електрозв’язку ITU-T L.1300 [4], загальні підходи до підвищення енергоефективності обробки навантаження ІКМ такі:

• підбір енергоефективного комп'ютерного та телекомунікаційного обладнання, його регулярна атестація (аудит);

• розгортання сервісів з використанням підходів віртуалізації;

• розробка ефективного програмного забезпечення;

• послуги з виведення з експлуатації невикористаного обладнання та зупинки

обладнання у разі простою;

• консолідація поточних послуг;

• постійний моніторинг енергоспоживання системи.

В роботі [5] запропоновано розподілити підходи щодо енергоефективної обробки навантаження на статичні та динамічні підходи. Статичні підходи не враховують динамічну змінюваність навантаження. Вдосконалення енергоефективності в динамічних підходах на рівні апаратного забезпечення – є складним та водночас дорогим для реалізації процесом, тому є доцільним вдосконалювати енергоспоживання на рівні програмного забезпечення.

Проведений огляд підходів щодо енергоефективного розподілу навантаження в ІКМ показав, що алгоритм енергоефективного планування навантаження Backfill більше підходить для вирішення задачі підвищення енергоефективності обробки даних з огляду на концепцію енерго-пропорційних розрахунків. Однак існує проблема вдосконалення Backfill з метою покращення його роботи в умовах недостатнього навантаження на систему, а також пошуку балансу між енергоефективністю та продуктивністю обробки даних в умовах помірного навантаження. Крім того, пропонується провести попередню сертифікацію кожного сервера кластера для отримання реальної залежності енергоспоживання від навантаження для кожного обчислювального вузла для індивідуального визначення моделі енергоспоживання кожної машини окремо. Однак ефективність цього підходу зменшується у випадку невисокої інтенсивності вхідного навантаження, оскільки він не забезпечує відсутність простою в умовах збитковості обчислювальних ресурсів.

Окремим виявленим недоліком існуючих методів є те, що жоден із них не вирішує задачу підвищення ефективності обслуговування навантаження з урахуванням усіх трьох виділених показників ефективності (енергоефективності, продуктивності та доступності системи), що є ключовими для обслуговування навантаження ІКМ.

Визначення проблеми та цілі дослідження. У дата центрах надається велика кількість послуг, що мають різні витрати енергоспоживання. Для обробки навантаження використовуються кластери. У залежності від задач вони можуть складатись з різних компонент, таких, як процесор, оперативна пам’ять, графічний процесор та жорсткий диск. Всі вони так, чи інакше використовуються електроенергію для їх роботи.

Тому основною метою є розробка програмне забезпечення, яке б дозволило:

знизити загальне споживання електроенергії, забезпечити дотримання вимог щодо SLA та збільшити енергоефективність обробки навантаження за рахунок збільшення кількості оброблених завдань, використовуючи ту саму кількість спожитої потужності.

Критерії ефективності запропонованого комплексного методу задаються специфікаціями та рекомендаціями Міжнародної спілки електрозв’язку та Європейського інституту телекомунікаційних стандартів, які визначають основні задачі, що формують обчислювальне навантаження сучасної ІКМ. Аналіз вимог щодо обслуговування цього навантаження дозволив виділити основні показники ефективності процесу обслуговування навантаження ІКМ: енергоефективність та продуктивність обслуговування, а також коефіцієнт готовності системи як показник її доступності. На основі цих показників сформульовано критерій ефективності обробки обчислювального навантаження в системі [6].

Енергоефективність обробки даних $\boldsymbol{E_\Sigma}$ – обсяг корисного навантаження ω обробленого системою (серверним кластером) з N вузлів при споживанні обсягу енергії W. При обробці навантаження в N вузлах сумарний обсяг енергії розраховується як $W = \sum_{j=1}^{N} W_j$, а енергоефективність обробки даних відповідно визначається як:

$$E_\Sigma = \frac{\omega}{\sum_{j=1}^{N} W_j} \; [\frac{FLOP}{\text{Вт*год}}]. \tag{1}$$

Чим більший цей показник, тим більш енергоефективною є система, оскільки вона може обробити більшу кількість навантаження при меншому обсязі спожитої енергії.

Продуктивність обробки даних $\boldsymbol{C_\Sigma}$ – це обсяг навантаження, що обробляється системою за одиницю часу:

$$C_\Sigma = \frac{\omega}{T} \; [\frac{FLOP}{c}], \tag{2}$$

де ω – обсяг корисного навантаження, що обробляється системою; T – час обробки.

Показник продуктивності фактично визначає швидкість обслуговування навантаження обчислювальною системою.

Коефіцієнт готовності системи p_{avail} як показник її доступності.

Коефіцієнт готовності в імовірнісному визначенні (тобто у випадку визначення його через математичні сподівання часу роботи та простою), пов'язаний з імовірністю втрати запиту згідно з виразом:

$$p_{avail} = 1 - p_{loss}. \quad (3)$$

Якщо з певних причин (наприклад, через відсутність вільних ресурсів обробки даних) запит було втрачено, він потребує повторної обробки, що негативно впливає на QoE [7], тобто якість клієнтського досвіду.

Сформулюємо ***критерій ефективності*** для досліджуваної системи. У теорії прийняття рішень критерій ефективності – це правило, що формується на основі вибраних показників ефективності та дозволяє зробити цілеспрямований вибір з множини альтернатив [8]. При цьому виділяють критерії оптимальності (що використовується для прийняття оптимальних рішень згідно з концепцією максимізації корисності) та критерій придатності (що використовується для прийняття задовільних рішень згідно з концепцією обмеженої раціональності).

З огляду на вищесказане, критерій оптимальності для досліджуваного процесу обслуговування навантаження в інформаційно-комунікаційній мережі визначимо у вигляді:

$$K_{opt} = E_{\Sigma} * C_{\Sigma} \rightarrow max, \quad (4)$$

при $p_{avail} \geq p_{avail_{SLA}}$.

Тобто у множині можливих конфігурацій системи обслуговування навантаження найбільш ефективною є така, що дозволяє отримати максимальне значення добутку показників енергоефективності E_{Σ} та продуктивності C_{Σ} при задовільному значенні коефіцієнта готовності системи p_{avail}. Задоволення критерію ефективності K_{opt} для кожного серверного кластера, що бере участь в обслуговуванні навантаження ІКМ (а саме, задач SDN та NVF, Network Slicing, Edge Computing та bDDN) позитивно впливає на продуктивність та енергоефективність інформаційно-комунікаційної мережі в цілому.

Короткий опис запропонованого підходу. Запропонований алгоритм обробки робочого навантаження складається з 4 основних кроків:

1) атестація та сортування вузлів;
2) визначення шаблонів масштабування;
3) горизонтальне масштабування та енергоефективне планування;
4) інтелектуальне прогнозування відхилень робочого навантаження та перебудова патернів.

На цих етапах ми прагнемо відповісти на такі питання відповідно:

1) Які обчислювальні вузли слід використовувати більш інтенсивно?
2) Скільки активних вузлів потрібно для обслуговування статистичного навантаження?
3) Як розподілити навантаження між поточними активними вузлами?
4) Як динамічно впоратися з відхиленнями робочого навантаження від статистистичного?

Експериментальний аналіз. Для визначення ефективності та працездатності розробленого програмного забезпечення було проведено натурний експеримент в одному з дата центрів НАН України .

Запропонований підхід було випробувано під час проведення натурного експерименту в одному з дата центрів України. Були змодельовані умови, під час яких надходить на обробку непередбачуваний вхідний потік заявок. Для опрацювання потоку використано 6 вузлів, а саме 3 фізичні та 3 віртуальні. Віртуальні вузли було створено з

використанням VirtualBox. На всіх вузлах встановлені дистрибутиви Linux. Один з комп'ютерів працював як головний вузол, що керує процесами розподілу та їх координуванням. Під час процесу підготовки відбувається встановлення необхідних програм, бібліотек та утиліт. Далі виконується налаштування мережі та розмежування прав доступу. Під час експерименту збирались необхідні для аналізу дані та заносились у файли формату .csv.

При аналізі результатів експерименту було визначено, що комплексний підхід у порівнянні з кожним показником по підвищенню ефективності дійсно забезпечує підвищення енергоефективності та демонструє гарний показних збереження потужності. Результати порівняння приведені в таблиці.

Таблиця 1. Результати порівняння.

Виграш за показником енергоефективності	9,953% порівняно з Backfill 26,382% порівняно з Round Robin
Виграш за показником продуктивності	5,593% порівняно з Backfill 49,458% порівняно з Round Robin
Виграш за показником доступності	-2,49% порівняно з Backfill 17,709% порівняно з Round Robin
Виграш за критерієм ефективності	15,722% порівняно з Backfill 88,887% порівняно з Round Robin при дотриманні вимог щодо доступності системи

Висновки. У даному дослідженні представлено ефективність комплексного методу підвищення енергоефективності та продуктивності програмного забезпечення розподілу навантаження у вузлах ІКМ при виконанні вимог щодо доступності системи обслуговування навантаження.

Література

1. Повторне калібрування оцінок використання енергії глобального центру обробки даних / E. Masanet et al. Наука. 2020. Vol. 367, no. 6481. P. 984–986. – Режим доступу до ресурсу: https://doi.org/10.1126/science.aba3758 (date of access: 03.07.2022).
2. Ринок ЦОД і технологічні тенденції. Презентація Power Electronics [Електронний ресурс] // Yole Développement, APEC. – 2016. – Режим доступу до ресурсу: https://www.slideshare.net/Yole_Developpement/data-center-market-and-technology-trends-power-electronics-presentation-held-at-apec-2016-from-yole-dveloppement.
3. Проблема з потужністю центрів обробки даних – Режим доступу до ресурсу: https://www.datacenterdynamics.com/es/features/el-problema-con-las-cifras-sobre-la-energ%C3%ADa-del-centro-de-datos/
4. Міжнародна спілка електрозв’язку. ITU-T L.1300 - Best practices for green data centres [Електронний ресурс] / Міжнародна спілка електрозв’язку. – 2014. – Режим доступу до ресурсу: https://www.itu.int/rec/T-REC-L.1300/en.
5. Надійність та енергоефективність у системах хмарних обчислень: Огляд і таксономія / Ю. Шарма та ін. Журнал мережевих і комп'ютерних програм. 2016. Vol. 74. P. 66–85. – Режим доступу до ресурсу: https://doi.org/10.1016/j.jnca.2016.08.010.
6. Оптимізація обчислень у дата-центрі за критерієм енергоефективності – Режим доступу до ресурсу: https://ela.kpi.ua/handle/123456789/39712
7. J. Berger QoS та QoE у мережах 5G Розвиток додатків і вимірювань : Семінар QSDG // Тестування мобільної мережі Rhode & Schwarz, Сінгапур, 19-21 August 2019.
8. Чижова, Є. Н. Управлінські рішення: навч. посібник/Є.М. Чижова, Д.Г. Сазонов, М.С. Чижов. - Білгород: Вид-во БДТУ, 2009. - 202 с.

УДК 004.4

КЕРУВАННЯ ОБЧИСЛЮВАЛЬНИМИ РЕСУРСАМИ КОРИСТУВАЦЬКИХ ПРИСТРОЇВ У СКЛАДІ КЛАСТЕРУ KUBERNETES

Смаглюк В.О., Алєксєєв М.О.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: amxleclerk@gmail.com, alexeyev@its.kpi.ua

MANAGEMENT OF COMPUTING RESOURCES OF USER DEVICES IN A KUBERNETES CLUSTER

The work is devoted to the topical issue of the effective use of computing resources in systems with a dynamic distributed architecture that use personal or public computing devices for the needs of distributed computing, specifically to the task of effectively managing the life cycle of working nodes of clusters of containerized applications. Unlike the known existing solutions, the systems considered in the work have a relatively short-term and non-deterministic lifetime of their computing agents and therefore must have specialized functionality for automatically connecting and disconnecting computing agents from the cluster, as far as the process of joining a new working node to a system takes time and requires a certain qualification and level of authorization. The approach proposed in the work is based on the designing of the process of managing working nodes in a form of Service Discovery in the Kubernetes cluster environment. The advantage of the proposed approach is the complete automation of the process based on prepared programs that include operations to check the user's operating environment, install the necessary software to connect to the computer system, or uninstall components and disable the agent at the user's request. The work considers the experimental environment, investigates the system's operation in possible use cases and justifies the effectiveness of the approach.

Для підвищення ефективності використання незайнятих ресурсів обчислювальних вузлів та зниження загального рівня їх простоювання і водночас, для вирішення нагальних завдань з розміщення та виконання програмних компонентів корпоративних інформаційно-обчислювальних систем у попередній роботі було вирішено створювати кластери із залученням персональних пристроїв користувачів, а також парку комп’ютерної техніки та загальнодоступних обчислювальних пристроїв у корпоративній мережі. Також було прийняте рішення щодо використання контейнеризації прикладних програм та програмної технології Kubernetes (далі – k8s) для оркестрації робочих навантажень на їх основі, оскільки цей підхід дозволяє використовувати апаратні і програмні обчислювальні ресурси різні за походженням і характеристиками, а також дає змогу підключати і від’єднувати їх у процесі експлуатації [1]. Вузол K8s (node, “нода”) або робочий вузол у даному контексті це фізична або віртуальна машина, яка

бере участь у кластері K8s, і яку можна використовувати для запуску робочих навантажень (pod, “под”) у вигляді контейнеризованих програм. Проте, процес долучення та від’єднання робочих вузлів потребує виконання певних операцій у ручному режимі. При невеликій кількості потенційних клієнтів адміністратор K8s кластеру може сам проконтролювати переходи між станами та виконувати конфігураційні задачі, а саме: ініціалізацію програмного забезпечення, аналіз відповідності наданого пристрою до вимог цільової системи або видалення його. Проте, зі збільшенням кількості робочих пристроїв N буде зростати операційне навантаження P на адміністративний вузол за певним експоненціальним законом $P = exp(N)$. Якщо додатково врахувати, що система є динамічною, тоді час життя робочих пристроїв не обов’язково буде збільшуватися за лінійним законом і треба відслідковувати та вести звітність про кожен з клієнтів: у якому стані вони знаходяться, а також які дії потрібно виконати, щоб безпечно перевести пристрій з одного в інший стан.

Враховуючи це, в рамках роботи пропонується ведення актуальної таблиці станів робочих пристроїв у вигляді Service Discovery, де у ролі сервіса виступають ноди, з використанням бази даних etcd, яка є розподіленим сховищем у форматі ключ-значення і зазвичай поставляється разом із K8s. Цей компонент зберігає всю інформацію про робочі навантаження, які представлені у системі, враховуючи облік нод. За допомогою інтерфейсу K8s API ця інформація періодично оновлюється, щоб відповідати реальному станові системи. Якщо у etcd немає інформації про певну з нод, тоді вважається, що вона перебуває у стані готовності до ініціалізації. Навіть у випадку, коли пристрій користувача було вилучено із кластеру, але програмні компоненти досі встановлено на його машині, він знову має пройти етап ініціалізації запиту на приєднання до розподільнювальної системи. Для автоматизації актуалізації інформації про робочі навантаження з використанням etcd та K8s API у роботі був створений автоматизований пакет (скрипт), який перевіряє систему на відповідність вимог цільової кластерної мережі, інсталює необхідні програмні пакети та приєднає клієнтський пристрій до K8s або навпаки здійснює від’єднання робочих вузлів (див. рис. 1).

Наведені сценарії контролюються створеним у роботі програмним кодом, що отримує клієнт із відповідної адреси. Проте, може бути ситуація, коли було втрачено зв’язок із робочим вузлом. У такому випадку, робочий вузол переводиться у стан «неактивний режим». Коли вузол вимикається або виходить з ладу, він переходить у стан NotReady, тобто його не можна використовувати для запуску подів. Після цього всі поди, запущені на вузлі,

стають недоступними. Робочі навантаження залишаються при цьому закріпленими за проблемним вузлом. Якщо K8s не може зв'язатися з вузлом, він чекає за замовчуванням 40 секунд, а потім встановлює статус вузла на Unknown. Якщо вузол залишається недоступним відбувається ініціювання «виселення» за допомогою API для всіх подів на недоступному вузлі. За замовчуванням контролер вузла чекає 5 хвилин між позначенням вузла як невідомого та поданням першого запиту на вилучення [3]. Якщо недоступний вузол не повернувся до мережі, його буде видалено із внутрішньої бази, що у термінах даної роботи означає переведення у стан "готовності до ініціалізації".

У випадку повторного приєднання втраченого робочого вузла після того, як його було видалено з K8s кластеру, клієнт повинен повністю пройти процес ініціалізації описаний вище (див. рис. 1,а).

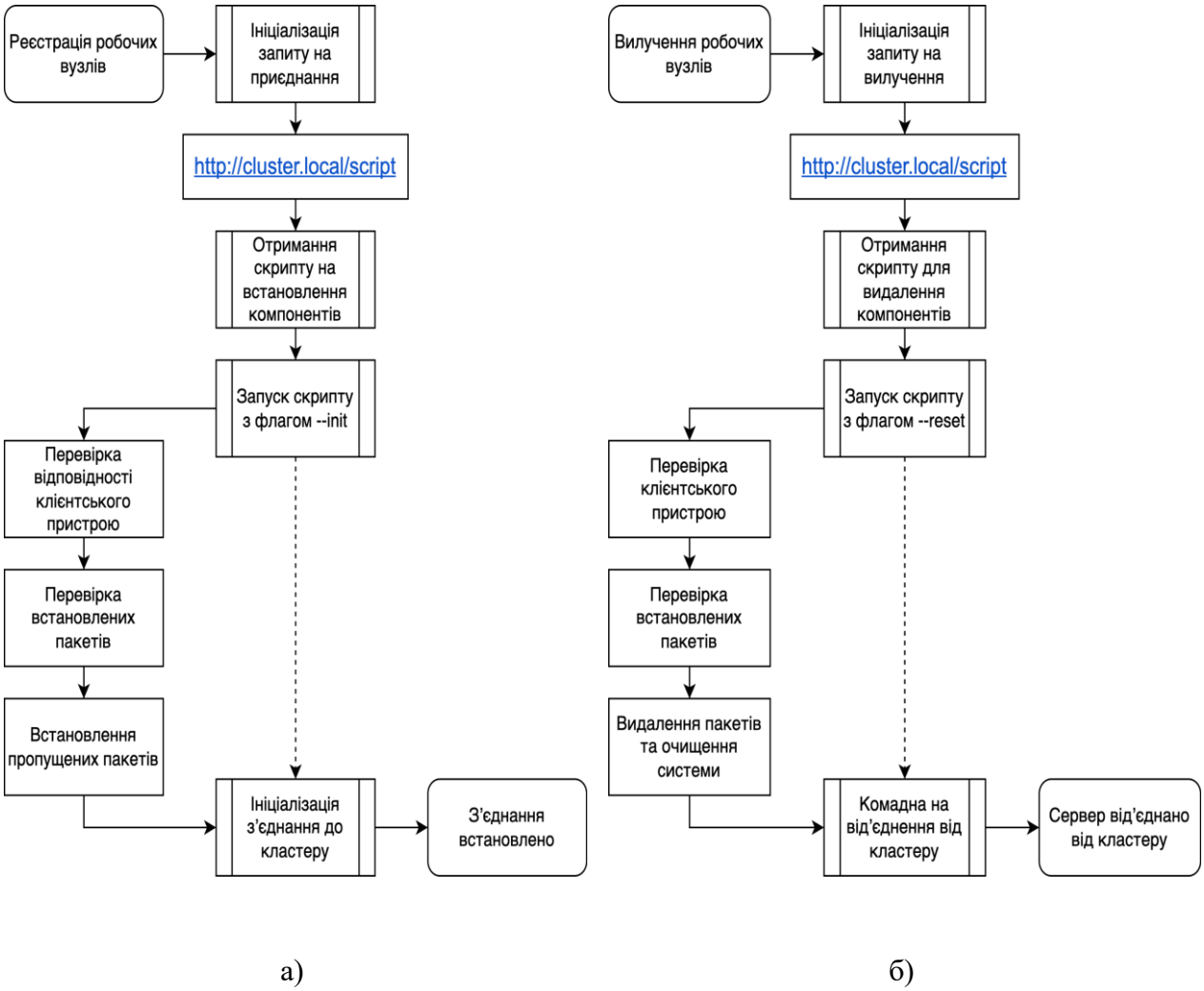
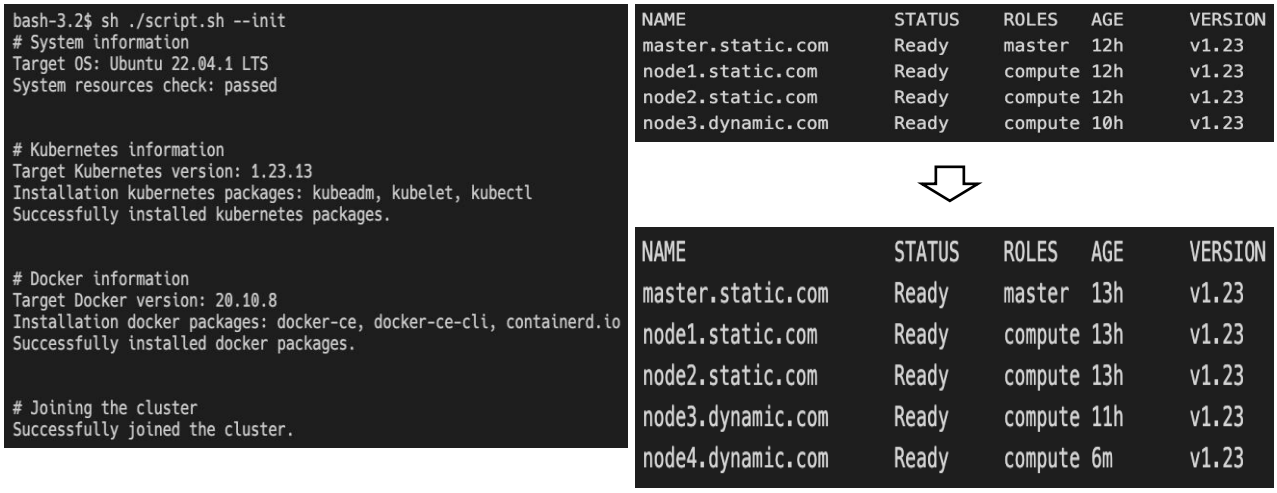


Рис. 1. Блок-схема процесу реєстрації а) від'єднання б) робочих вузлів

У роботі був створений експериментальний макет (див. рис. 2), який

містить один головний вузол, два робочі статичні вузли, один динамічний вузол (у стані “активний режим”), потенційний динамічний вузол (у стані “готовність до ініціалізації”) та точку доступу (в рамках корпоративної мережі) з виконувальним програмним кодом. Результат роботи розробленого ПЗ показаний на рис. 2.



а) б)

Рис. 2. Реєстрація нового вузла а) та оновлений перелік б) робочих вузлів.

Висновки.

1. Завдяки програмному коду вдалося мінімізувати оперативне навантаження на адміністратора K8s кластеру, стосовно управління життєвим циклом робочих вузлів та їх підготовкою до приєднання у систему.

2. Запропонований метод дозволяє автоматизувати процес реєстрації та вилучення робочих вузлів до K8s кластеру, що дає можливість побудувати динамічну обчислювальну систему з робочими вузлами з короткостроковим і недетермінованим часом життя своїх обчислювальних агентів.

Література

1. Смаглюк В.О., Алєксєєв М.О. Керування клієнтськими обчислювальними ресурсами з динамічним життєвим циклом у корпоративній мережі. ISSN 2788-5518. Інфокомунікаційні та комп’ютерні технології: Науковий журнал. № 2(04) 2022. К.: Університет "Україна", 2022. - с.134-142
2. Etcd Documentation. “What is etcd?”: Онлайн: https://etcd.io/docs/v3.5/faq/#what-is-etcd: 25.03.2022.
3. Kubernetes Docs. Kubernetes Nodes: Conditions: Онлайн: https://kubernetes.io/docs/concepts/architecture/nodes/#condition: 22.03.2022 17:43.

УДК 004.94

ТРАНСДИСЦІПЛІНАРНИЙ ПІДХІД ДО ВИСВІТЛЕННЯ МУЗЕЙНИХ АРТЕФАКТІВ НА БАЗІ ОНТОЛОГІЙ

Кудляк В.М.[1], Бєлан Т.І.[1], Новогрудська Р.Л.[1,2]
[1] НЦ «Мала академія наук України»,
[2] *Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна*
E-mail: masterds56@gmail.com, t.belan08@gmail.com, rinan@ukr.net

A TRANSDISCIPLINARY APPROACH TO THE ILLUMINATION OF MUSEUM ARTIFACTS BASED ON ONTOLOGIES

The research proposes a transdisciplinary approach to the development of modern educational and cultural Internet portals. Innovative possibilities, methods and technologies for the development of multidimensional structured information Internet sites presenting information about cultural heritage objects based on ontologies are described on the example of a created and actually operating web-portal “Museum planet”.

На сьогоднішній день спостерігається стрімкий розвиток різноманітних веб-ресурсів, які надають доступ до інформації різного роду. Серед таких ресурсів можна виділити широкий пласт культурно-історичних сайтів та порталів, які відображають інформацію про об’єкти культурної спадщини людства загалом, та нашої країни зокрема. Їх затребуваність значно зросла у останні роки. У період пандемії та режиму правового військового стану, саме такі ресурси дозволяють реалізовувати відображення та ознайомлення з історичними та культурними об’єктами в он-лайн форматі.

Віртуальні музеї, бібліотеки, туристичні центри в сучасному світі є зручним форматом послуг для ефективного та швидкого доступу до інформації з використанням інтернет-технологій. Вони стали незамінні при проведенні презентацій, виставок, віртуальних екскурсій, тому що проектуються із залученням сучасних когнітивних і соціальних технологій, а також трансферу знань. Основною вимогою до формування їхньої структури є продуманий комплексний трансдисціплінарний підхід, глибина і різнобічність розкриття тематичних напрямів та наявність інтерактивного програмного забезпечення.

Деякі сучасні дослідження детально описують основні принципи розробки віртуальних музеїв. Так, наприклад [1] надає короткий опис принципів функціонування віртуальних музеїв, а також проблем, які виникають при їх розробці. У дослідженні [2] наведено опис віртуального середовища, яке надає доступ одразу до 10 музеїв, зображена структура бази даних такого музейного простору та додатку для роботи з такою базою, а також описані характеристики та дизайн запропонованого середовища.

У представленому дослідженні наведено трансдисціплінарний підхід до розробки сучасних освітньо-культурних сайтів. На прикладі створеного та реально діючого веб-порталу описані інноваційні можливості, методики та

технології розробки багатовимірних структурованих інформаційних сайтів для представлення інформації про об’єкти культурної спадщини на основі онтологій [3].

Онтології є одним з підходів до структурованого представлення певної предметної галузі. Перевагою онтологій як способу представлення знань є формальна структура, яка спрощує їх комп'ютерну обробку. Онтологія може бути представлена як трійка **Ошибка! Источник ссылки не найден.** [4]:

$$O = \langle X, R, F \rangle \qquad (1)$$

На практиці часто виникає потреба інтерактивної взаємодії з інформацією, що міститься в онтологіях. Таку взаємодію можна забезпечити з допомогою інтерактивних онтологічних документів виду **Ошибка! Источник ссылки не найден.**:

$$\langle O_I, O_\Sigma, N \rangle \qquad (2)$$

де O_I, O_Σ – інформаційна і керуюча онтології відповідно; N – натуральна система, що забезпечує інтерактивну взаємодію з вмістом O_I з використанням описаних в O_Σ функцій.

Натуральна система, що входить до складу інтерактивного документа, може бути умовно представлена у вигляді певної функції (цільової функції) вигляду **Ошибка! Источник ссылки не найден.**:

$$f_N(\breve{x}_1 ... \breve{x}_n) = \breve{Q}_n(Q_{n-1}(...Q_1(O, \breve{x}^1)..., \breve{x}^{n-1}), \breve{x}^n) \qquad (3)$$

де $\breve{x}_i$ – команди користувача, тобто дії, які він виконує в процесі інтерактивної взаємодії з інформацією; O – набір інформації, якою оперує система в певний момент, у формі онтології; Q_i – функції обробки інформації; $\breve{Q}_n$ – функція відображення, результатом якої є власне надана користувачу інформація в текстовій або графічній формі.

Модифікуючи множину функцій Q_i, можна створювати додатки під конкретні потреби тих чи інших користувачів. Саме таке онтологічне представлення використовується для представлення інформаційних ресурсів порталу «Музейна планета».

«Музейна планета» [5] — це новітній інформаційний портал, що не тільки сприяє систематизації набутих знань, а й допомагає формуванню інформаційної культури учнів на основі навчальних досліджень культурно-історичної спадщини нації, визначення її вкладу у розвиток світової культури. Сама ідея порталу є одним із шляхів реалізації концепції запровадження національно-патріотичного виховання, формування культури мислення, розвитку творчих та дослідницьких здібностей учнівської молоді. Загальний вигляд онтологічного порталу показано на рисунку 1.

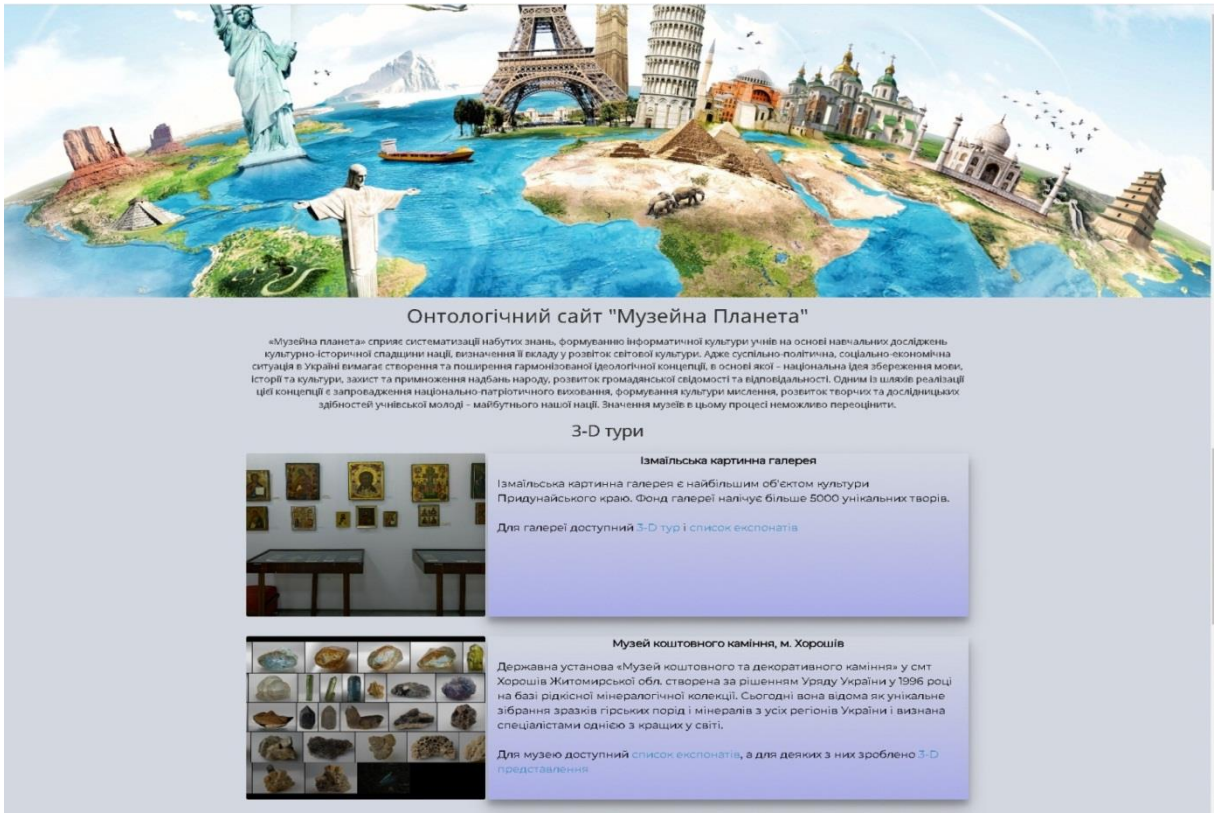


Рис. 1. Загальний вигляд онтологічного порталу.

Для розробки порталу були використані багатофункціональні технології DeepZoom, OpenSeaDragon, PivotViewer та цілий ряд оригінальних алгоритмів, які були інтегровані в середовище інтерактивного документу як спеціалізовані функції обробки і відображення інформації через представлення а рівні онтології. У комбінації з широкими можливостями онтологій щодо опису елементів предметної галузі це надало можливість всебічного представлення реальних музейних артефактів усіма засобами прогресивних технологій відображення реальних матеріальних предметів та їх особливостей.

Література

1. Han Y. On the construction of virtual museum. IOP Conference Series: Earth and Environmental Science. 2020. Vol. 510. P. 062034. DOI: 10.1088/1755-1315/510/6/062034.
2. Charitos D., Lepouras G., Vassilakis C., Vivi K., Leda H. An Approach to Designing and Implementing Virtual Museums. Proc. 7th International UK VR-SIG Conference. 2003. P. 1-8.
3. Кудляк, В., Бєлан, Т., Пархоменко, О., Новогрудська, Р., & Савченко, Я. (2022). ТРАНСДИСЦИПЛІНАРНИЙ ПІДХІД У ВИСВІТЛЕННІ МУЗЕЙНИХ АРТЕФАКТІВ ЗАСОБАМИ СУЧАСНИХ КОГНІТИВНИХ ТЕХНОЛОГІЙ. Наукові записки Малої академії наук України, (3(25), 80–90. https://doi.org/10.51707/2618-0529-2022-25-09
4. R. Novogrudska and M. Popova, "A Compehencive Review of Ontology-based Information Systems for Educational Process Support," 2021 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Odesa, Ukraine, 2021, pp. 76-79, doi: 10.1109/UkrMiCo52950.2021.9716675.
5. Онтологічний сайт «Музейна планета». [Електронний ресурс] — Режим доступу: https://museum.ulif.org.ua

УДК 81`33 + 004.82 + 004.91

ОНТОЛОГОКЕРОВАНІ КОГНІТИВНІ СЕРВІСИ ЯК СКЛАДОВА ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ АНАЛІЗУ СТАТИСТИЧНОЇ ІНФОРМАЦІЇ

Приходнюк В. В., Горборуков В. В.
Національний центр «Мала академія наук України»,
tangens91@gmail.com, slavon07@gmail.com

ONTOLOGICAL COGNITIVE SERVICES AS A COMPONENT OF INFORMATION AND TELECOMMUNICATION SYSTEMS ANALYSIS OF STATISTICAL INFORMATION

In the operation of most information and telecommunication systems, there is a need to use various data, in particular, represented by natural language documents. To effectively operate with them, it is advisable to use modern cognitive services, especially ontology-controlled ones. This paper proposes the use of such a cognitive toolkit that implements the recursive reduction method and is an effective modern solution.

Згідно українського законодавства [1], інформаційно-телекомунікаційною системою вважається організаційно-технічна сукупність, що складається з автоматизованої системи та мережі передачі даних. Створення інформаційно-телекомунікаційних систем є надзвичайно складним процесом, що часто може бути зв’язаним з використанням великої кількості різнорідних засобів, модулів та інструментів.

В залежності від призначення інформаційно-телекомунікаційної системи, при її функціонуванні може виникати потреба у внесенні різноманітних даних, представлених природномовними документами. Часто об’єми таких даних є настільки великими, що внесення їх вручну може бути недоцільним або навіть неможливим. В таких випадках можуть використовуватись сучасні когнітивні сервіси, зокрема – онтологокеровані [2, 3]. Особливо гостро стає така задача при аналізі статистичної інформації, що часто представлена великими масивами слабкоструктурованих документів. Такі масиви в загальному випадку досить легко піддаються автоматизованій обробці, зокрема – за допомогою розробленого методу рекурсивної редукції [2].

Даний метод передбачає використання спеціалізованих онтологій (онтологічних дескрипторів структуризації) для опису перетворень, що повинні застосовуватись до вхідного слабко структурованого масиву даних. Метод застосовується до кожного з документів в рамках вхідного масиву

даних і передбачає [2] виконання послідовності перетворень **Ошибка! Источник ссылки не найден.**.

$$T \to T_{sn} \to T_{mk} \to \langle X, T_{mk} \rangle \to \langle X, R, T_{mk} \rangle \to \langle X, R, F, T_{mk} \rangle \to O \qquad (4)$$

де T – текст вхідного природномовного документу; T_{sn} – лексична структура тексту; T_{mk} – розширена лексична структура; X, R, F – множини об'єктів, зв'язків і функцій інтерпретації вихідної онтології O.

Основою перетворення **Ошибка! Источник ссылки не найден.** є база правил рекурсивної редукції, що отримується в результаті інтерпретації онтологічного дескриптора структуризації. Кожне з правил в базі має вигляд **Ошибка! Источник ссылки не найден.**, і складається з двох функцій – ідентифікації та перетворення.

$$d = \langle f_{id}^{d}, f_{tr}^{d} \rangle, \qquad (5)$$

де f_{id}^{d} – функція ідентифікації лексем; f_{tr}^{d} – функція перетворення лексем.

$$F_{rd}(\beta_L, D) = \begin{cases} f_{tr}^{d}(\beta_0), \exists d \in D, f_{id}^{d}(\beta_0) \\ F_{rd}(\beta_L \setminus \beta_0, D) \end{cases} \qquad (6)$$

де β_L – множина всіх підмножин, сформована для певної множини лексем L; D – база правил виду **Ошибка! Источник ссылки не найден.**; f_{id}^{d}, f_{tr}^{d} – елементи певного правила d.

Прикладом дескриптора структуризації є онтологія, що задає процес створення обробки статистичних даних щодо кадрового забезпечення установ НАН України (Рис. 1).

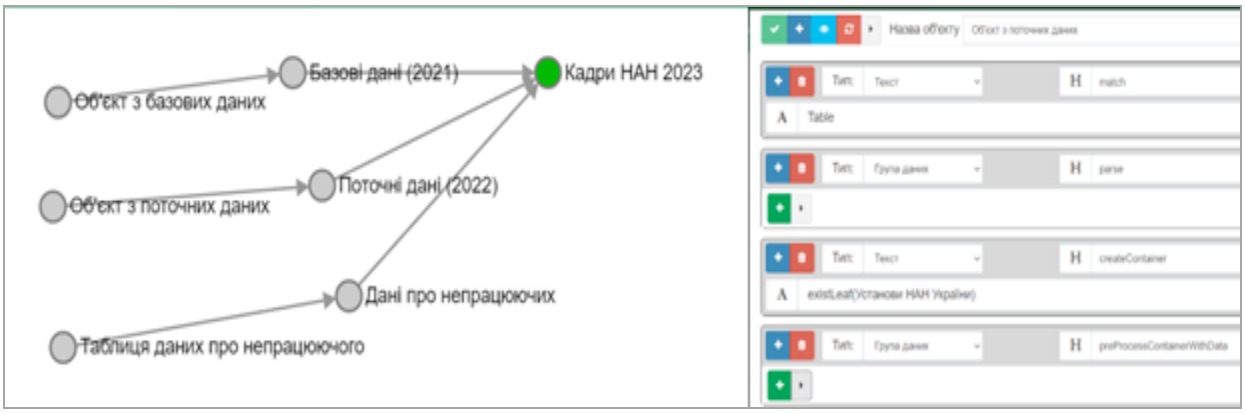


Рис. 1. Приклад онтологічного дескриптора структуризації.

Такий дескриптор може використовуватись для наповнення даними автоматизованих робочих місць в рамках певного мережевого середовища (Рис. 2), призначеного для роботи експертів.

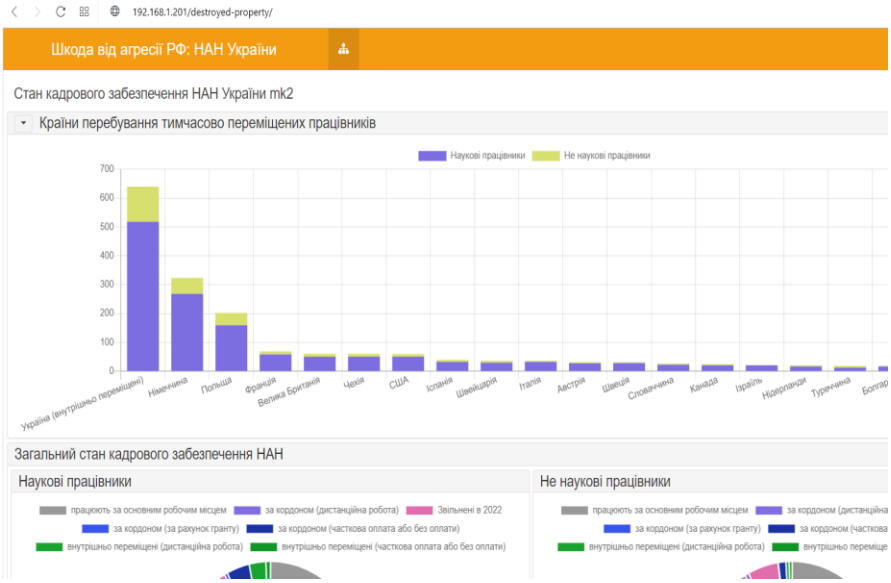


Рис. 2. АРМ відображення результатів в рамках локального мережевого середовища

Інструментарій, що реалізує метод рекурсивної редукції, може легко інтегруватись в різноманітні інформаційно-телекомунікаційні системи, як відкриті (з доступом з мережі Інтернет) так і закриті. В залежності від розгорнутої в рамках системи інфраструктури інструментарій може працювати як локально (на робочому місці оператора системи) так і в рамках певного виділеного серверу (серверу додатків). Онтології, що керують роботою інструментарію, також можуть розміщуватись як локально (в файловій системі робочого місця або серверу), так і в рамках виділеного серверу онтологій (серверу КІТ «ПОЛІЕДР»).

Запропонований інструментарій є ефективним сучасним рішенням, що дозволяє суттєво зменшити витрати часу операторів інформаційно-телекомунікаційних систем, зокрема, таких, що призначені для аналізу статистичної інформації.

Література

1. Наказ “Про затвердження Порядку захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах” від 24.12.2001 N 76. URL: https://zakon.rada.gov.ua/laws/show/z0027-02#Text
2. Stryzhak O., Prykhodniuk V., Popova M., Nadutenko M., Haiko S., Chepkov R. Development of an Oceanographic Databank Based on Ontological Interactive Documents. Lecture Notes in Networks and Systems. Cham : Springer. 2021. С. 97–114. DOI: https://doi.org/10.1007/978-3-030-80126-7_8
3. Nadutenko M., Prykhodniuk V., Shyrokov V., Stryzhak O. Ontology-Driven Lexicographic Systems. Advances in Information and Communication. FICC 2022. Lecture Notes in Networks and Systems. Cham : Springer. 2022. С. 204–215. DOI: https://doi.org/10.1007/978-3-030-98012-2_16

УДК 004.62:004.93:004.72

АНАЛІЗ ТА ПОРІВНЯННЯ МЕТОДІВ ОБРОБКИ ГРАФІЧНОЇ ІНФОРМАЦІЇ В МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ

Курдеча В.В., Любарска С.І.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: lovejapancat1@gmail.com

ANALYSIS AND COMPARISON OF GRAPHIC INFORMATION PROCESSING METHODS IN THE INTERNET OF THINGS NETWORK

A list of problems in the transmission and processing of graphic information in the Internet of Things network has been created.

Обробка графічної інформації носить принциповий характер для розвитку мережі Інтернету речей. При цьому виявлено ряд проблем описаних в даній публікації. Характерною рисою цих проблем є наявність протиріч при побудові подібних систем та реалізації процесу обробки графічної інформації зокрема, що і обумовлює актуальність даної проблематики.

1) Обробка графічної інформації в IoT може здійснюватися за допомогою різноманітних методів.

До існуючих засобів обробки графічної інформації в IoT можна віднести наступні:

1. Computer vision tracking: це програмний засіб який виявляє обєкти, а потім відстежує їх переміщення.

Ця технологія потребує спеціалістів. Коли пристрій виходить з ладе через вірус або інші проблеми, може статися збій в обробці зображення.

2. Image data analysis: дозволяє витягувати значущу інформацію із цифрових зображень за допомогою технологій обробки цифрових зображень.

Це дуже трудомістко і дорого в залежності від конкретної системи.

3. Pattern recognition: цей засіб дозволяє автоматизоване розпізнавання шаблонів і закономірностей у даних.

Ця технологія складна у виконанні і надзвичайно повільна, також розпізнавання вимагає більшого набору даних, щоб отримати підвищену

точність

4. Virtual reality: це засіб імітації досвіду, який використовує відстеження пози та 3D-дисплеї поблизу очей, щоб дати користувачеві відчуття занурення у віртуальний світ.

Ця технологія взагалі не підходить для вирішення проблем, які розглядаються(рис.1).

2) Проблеми обробки графічної інформації в IoT.

1. Графічна інформація зазвичай містить великий обсяг даних, що може становити проблему при зберіганні та передачі її через мережу IoT.

2. Зображення можуть бути зняті з різною якістю, або можуть бути викривлені під час передачі через мережу. Це може призвести до складнощів у визначенні деталей та характеристик зображення.

3. У IoT-пристроях може бути обмежена можливість обробки даних, що може змінити точність результатів обробки графічної інформації.

4. Збір і передача графічної інформації можуть бути пов'язані з питаннями безпеки, такими як можливість несанкціонованого доступу до інформації.

5. Існує ризик, що графічна інформація може бути зібрана різними IoT-пристроями, які можуть використовувати різні формати файлів або протоколи зв'язку. Це може створити проблеми з обробкою та аналізом даних.

Рис.1. Існуючі проблеми з обробкою графічної інформації в IoT.

3) Методи обробки графічної інформації в IoT:

1. Компресія даних: компресія даних може допомогти зменшити розмір зображення та скоротити час передачі даних через мережу IoT.

2. Використання алгоритмів обробки зображень: існують різні

алгоритми обробки зображень, такі як виявлення контуру, сегментація зображень та класифікація зображень.

3. Використання штучного інтелекту: штучний інтелект може бути використаний для вирішення проблем з обробкою графічної інформації.

4. Застосування захисту даних: для забезпечення безпеки даних, що передаються через мережу IoT, можна використовувати різні методи захисту, такі як шифрування даних та аутентифікація користувачів.

5. Стандартизація даних: стандартизація форматів зображень та протоколів зв'язку може допомогти вирішити проблему сумісності між різними IoT-пристроями.

Рис.2. Методи вирішення проблем з обробкою графічної інформації в IoT.

В публікації було сформовано перелік проблем що виникають під час обробки графічної інформації в мережі IoT, а також проаналізовано існуючі методи які застосовуються в даній сфері.

На основі сформованого переліку методів в подальшому планується створення модифікованого методу обробки графічної інформації.

Література

1. Комп'ютерний зір: особливості та переваги технології [Електронний ресурс] – Режим доступу до ресурсу: https://zt-news.org.ua/index.php?newsid=18800.
2. Технологія комп’ютерного зору: типові помилки під час розробки та впровадження [Електронний ресурс] – Режим доступу до ресурсу: https://brainberry.ua/uk/newsroom/blog/computer-vision-technology-common-mistakes.
3. IMAGE PROCESSING ADVANTAGES AND DISADVANTAGES: A STUDY [Електронний ресурс] – Режим доступу до ресурсу: http://www.ijcea.com/wp-content/uploads/2018/05/Suresha.pdf.
4. Advantages and disadvantages of pattern recognition [Електронний ресурс] – Режим доступу до ресурсу: http://way2benefits.com/advantages-and-disadvantages-of-pattern-recognition/.
5. Virtual Reality Advantages And Disadvantages | What is Virtual Reality (VR)?, Benefits, Drawbacks, Pros and Cons [Електронний ресурс] – Режим доступу до ресурсу: https://www.aplustopper.com/virtual-reality-advantages-and-disadvantages/.
6. J. Yamnenko, L. Globa, V. Kurdecha and A. Zakharchuk, "Data Processing in IoT Systems based on Fuzzy Logics," 2019 Modern Electric Power Systems (MEPS), Wroclaw, Poland, 2019, pp. 1-4, doi: 10.1109/MEPS46793.2019.9395055.

УДК 004.62:004.031.2:004.031.43

ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖІ ІНТЕРНЕТ РЕЧЕЙ

Бушинський Д.А., Курдеча В.В.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: dbushynskyi2002@gmail.com

CHALLENGES OF INFORMATION SECURITY IN THE INTERNET OF THINGS NETWORK

Suggestions for improving the effectiveness of protection and integrity of confidential data by modifying the architecture of the Internet of Things network.

Конфіденційність є дуже широким і різноманітним поняттям, для якого в літературі пропонується безліч визначень і точок зору. Інформаційну конфіденційність прийнято розуміти як право та можливість обирати, яка особиста інформація буде відома і кому саме. Таке визначення конфіденційності, охоплює ідею інформаційного самовизначення, дозволяючи користувачеві оцінити ризики, вжити відповідних заходів для захисту своєї інформації та бути впевненим, що вона не виконується за межами сфери його безпосереднього контролю.

Поняття особистої інформації є нечітким, оскільки конфіденційність є глибоко соціальною концепцією, що підлягає дуже різноманітним індивідуальним сприйняттям і вимогам. Тож, при розробці нових систем і послуг необхідно ретельно оцінити чутливість залученої інформації та відповідних вимог користувачів.

З вдосконаленням пристроїв, збільшенням обчислювальної потужності та зменшенням споживання енергії тенденція впровадження IoT продовжиться. Однією з найскладніших тем у такому взаємопов’язаному світі мініатюрних систем і датчиків є аспекти безпеки та конфіденційності: без упевненості, що гарантується безпека приватної інформації та належний захист, користувачі не за хочуть прийняти цю нову технологію, яка непомітно інтегрується в життя. Щоб широко запровадити IoT, цю проблему слід вирішити, щоб забезпечити впевненість користувачів щодо конфіденційності та контролю особистої інформації.

Ця публікація присвячена проблемам безпеки, конфіденційності та методам їх вирішення в мережі IoT. Уразливі місця, як правило, відносяться до мало захищених місць системи, якими можуть зацікавитися зловмисниками для виконання корисливих дій. В Інтернеті речей хакери можуть використовувати цілісність, конфіденційність і доступність послуг для законних користувачів, користуючись перевагами таких проблем, що проростають. Тому розуміння такої делікатності в системі стає обов'язковим до розробки відповідних захисних механізмів.

Для початку потрібно вказати зображені на рис. 1 основні вразливості IoT:

1. Безпека пристроїв.

Цей аспект безпеки в першу чергу включає фізичне пошкодження пристроїв IoT, головним чином спричинене несанкціонованим доступом до них.

2. Незахищене впровадження.

Відсутність належної перевірки перед впровадженням пристрою.

3. Мережеві вразливості.

Зазвичай вони включають незахищені служби в самих пристроях, відсутність належної автентифікації та шифрування, тобто використання стандартних або слабких паролів, а також застосування методів шифрування, які не відповідають стандартам полегшеної криптографії в IoT

4. Уразливості програмного забезпечення.

Невиконання відповідних оновлень програмного забезпечення, використання застарілих бібліотек або компонентів програмного забезпечення.

5. Недостатня конфіденційність.

Це означає компрометацію особистої інформації користувача без запиту його дозволу.

6. Недосконалий механізм аудиту.

Відсутність достатнього механізму журналювання.

Рис. 1. Основні вразливості IoT.

Рішення на основі навчання для захисту IoT. Фахівці з machine learning (далі - ML) визначають підходи до навчання як продуктивний інструмент для вирішення проблем безпеки, що призводить до

об'єднання підходів ML і deep learning (далі - DL) з технологією intrusion detection system (далі – IDS).

Контрольоване навчання.

Процедура вивчення функціональних можливостей із навчального набору даних. Основною метою є оцінка функції відображення для прогнозування правильних вихідних міток для заданих нових даних.

Неконтрольоване навчання.

Для моделювання елементарної або прихованої структури даних через відсутність позначеного набору даних сприяє комплексній оцінці даних.

Навчання з підкріпленням.

Методика пов'язана із застосуванням відповідних дій програмних агентів у середовищі для максимізації роботи. Два основні методи навчання з підкріпленням включають пошук політики та апроксимацію функції цінності.

Федеративне навчання.

Ця передова техніка машинного навчання здатна тренувати моделі машинного навчання розподіленим способом. Традиційно під час передачі оновлень між централізовано керованим сервером і підключеними пристроями в мережі спостерігалися значні витрати на зв'язок. Накладні витрати на мережу призводять до компрометації швидкості передачі даних, надійності, конфіденційності та управління ресурсами. Проте з появою методів федеративного навчання (далі – FL) спостерігається значне покращення аспекту безпеки розумних систем. Моделі навчання під FL використовують переваги розподіленого характеру навчання та забезпечують передачу лише параметрів, які можна вивчати, замість цілих наборів даних.

Для прикладу, розглядаючи «розумне місто» де пристрої знаходяться на відкритій території, тобто, повністю залишені у розпорядженні природи та зловмисників, доцільно використати як доповнення захисту до вище згаданого ML та DL програмне забезпечення (далі - ПЗ) яке зможе моніторити стан кожного пристрою в мережі. Це у свою чергу завадить клонуванню пристроїв, несанкціонованому доступу до них. Забезпечення конфіденційності базуватиметься не лише на зібраній інформації від ПЗ про певні аномалії конкретного пристрою, а й на передачі цих даних для опрацювання ML для постійного вдосконалення захисту.

Література

1. Jan H. Z. Конфіденційність в Інтернеті речей: загрози та виклики [Електронний ресурс] / H. Z. Jan, G. M. Oscar, W. Klaus – Режим доступу до ресурсу: https://onlinelibrary.wiley.com/doi/epdf/10.1002/sec.795.
2. Wei C. H. Інтернет речей: еволюція, проблеми та складнощі безпеки [Електронний ресурс] / C. H. Wei, M. Parushi, S. Yashwant – Режим доступу до ресурсу: https://www.mdpi.com/1424-8220/21/5/1809.
3. Fadele A. A. Безпека Інтернету речей: огляд [Електронний ресурс] / A. A. Fadele, O. Mazliza, A. T. brahim – Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/abs/pii/S1084804517301455.

УДК 004.7:621.316:620.9

ЕНЕРГЕТИЧНЕ ПРОГНОЗУВАННЯ ТА УПРАВЛІННЯ З ПІДТРИМКОЮ ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ ГІБРИДНИХ МІКРОМЕРЕЖ

Корнійчук І. Г., Курдеча В.В.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: korniichuk2002@gmail.com

ENERGY FORECASTING AND MANAGEMENT WITH THE SUPPORT OF THE INTERNET OF THINGS FOR HYBRID MICRO-GRIDS

Using machine learning and artificial intelligence algorithms to forecast energy demand and optimize energy production and storage accordingly.

Енергетика є однією з ключових галузей людства. На разі з розвитком «зелених» технологій особливого значення отримали гібридні мікромережі. Проте через складність функціональності та розширення гібридних мікромереж зростає попит в правильному прогнозуванні та швидкому управлінні енергією.

Мета цього дослідження полягає в тому, щоб вивчити потенціал інтеграції Інтернету речей (IoT) у гібридні мікромережі для покращення прогнозування та управління енергією. Це буде досягнуто завдяки використанню алгоритмів машинного навчання та штучного інтелекту для прогнозування попиту на енергію та відповідної оптимізації виробництва та зберігання енергії.

Інтеграція IoT у гібридні мікромережі та використання алгоритмів машинного навчання та штучного інтелекту для прогнозування попиту на енергію та оптимізації виробництва та зберігання енергії призведе до підвищення енергоефективності та економії коштів. IoT дозволить збирати дані в реальному часі та аналізувати моделі споживання енергії, що сприятиме точному прогнозуванню попиту на енергію.

Метод інтеграції IoT у гібридні мікромережі передбачає розгортання датчиків і інтелектуальних пристроїв у всій мікромережі для збору даних у режимі реального часу про споживання, виробництво та зберігання енергії. Потім ці дані передаються в централізовану систему (рис. 1), яка використовує алгоритми машинного навчання та штучного інтелекту для аналізу даних і прогнозування майбутнього попиту на енергію.

Інтеграція IoT в гібридні мікромережі привернула значну увагу в останні роки - наприклад, Al-Ammar E. та ін. (2020) розробили прогностичну модель для попиту на енергію за допомогою алгоритмів машинного навчання, яка показала точність 95%. Так само Khodayari A. та ін. (2019) використали алгоритм глибокого навчання для оптимізації виробництва та зберігання енергії в гібридній мікромережі, що призвело до зниження витрат на енергію на 23%.

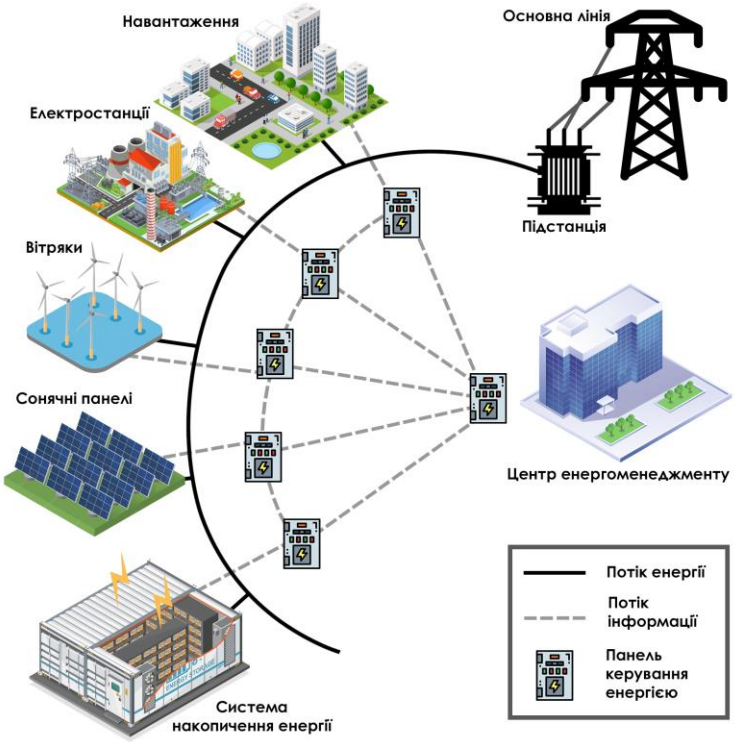


Рис. 1. Схема експорту та імпорту енергії.

Експорт та імпорт відновлюваної енергії з підтримкою інтернету речей для гібридних мікромереж може бути досягнутий за допомогою наступних кроків (рис. 2):

Рис. 2. Ключові стратегії експорту та імпорту відновлюваної енергії за допомогою гібридних мікромереж на основі IoT.

- Моніторинг виробництва та споживання енергії в режимі реального часу для визначення періодів надлишкового виробництва енергії на експорт.
- Енергетичне прогнозування з використанням історичних даних і моніторингу в реальному часі для планування експорту або імпорту енергії.
- Оптимізація накопичення енергії за допомогою батарей, керованих IoT, для зниження витрат і оптимізації використання енергії.

- Підключення до основної або сусідніх мікромереж для полегшення імпорту або експорту енергії.

- Впровадження програми реагування на попит за допомогою пристроїв IoT для зменшення пікового навантаження та збільшення доступної енергії для експорту.

- Розумні контракти для ефективної та точної торгівлі енергією між мікромережами та основною мережею.

- Видача кредитів на відновлювану енергетику з використанням IoT-моніторингу виробництва та споживання енергії для заохочення виробництва та споживання відновлюваної енергії.

Ці заходи оптимізують використання енергії та зменшують втрати, зробивши відновлювану енергію доступнішою для споживачів.

Для оптимізації виробництва та зберігання енергії система використовує прогнозований попит для визначення оптимальної комбінації джерел енергії та систем зберігання. У періоди високого попиту система отримує енергію з кількох джерел, включаючи сонячні батареї, вітряні турбіни та системи зберігання енергії, щоб забезпечити надійне та стабільне енергопостачання.

Крім того, система також може динамічно регулювати виробництво та накопичення енергії на основі зміни погодних умов і моделей попиту на енергію.

Інтеграція IoT і алгоритмів машинного навчання в гібридні мікромережі пропонує значний потенціал для підвищення енергоефективності та досягнення економії коштів. Збір даних у режимі реального часу та аналіз моделей споживання енергії, точне прогнозування попиту на енергію та ефективне використання енергетичних ресурсів є одними з переваг цієї технології. Необхідні подальші дослідження, щоб вивчити весь потенціал цієї технології та визначити шляхи оптимізації її використання в гібридних мікромережах. Проте результати показують, що ця технологія є перспективною для створення більш сталого енергетичного майбутнього.

Література

1. Al-Ammar, E., Al-Ammar, M., Al-Fahad, A., & Alsulaiman, A. (2020). A predictive model for energy demand in a hybrid microgrid using machine learning algorithms. Energies, 13(20), 5439.
2. Khodayari, A., Nazari-Heris, M., & Parastegari, S. (2019). A deep learning-based approach for energy management in a hybrid microgrid. Journal of Energy Storage, 23, 29-39.
3. Ma, Y., Zhao, J., Zou, J., & Xu, Z. (2020). Predictive control of energy management for a hybrid microgrid using a deep neural network. Journal of Energy Storage, 30, 101474.
4. J. Yamnenko, L. Globa, V. Kurdecha and A. Zakharchuk, "Data Processing in IoT Systems based on Fuzzy Logics," 2019 Modern Electric Power Systems (MEPS), Wroclaw, Poland, 2019, pp. 1-4, doi: 10.1109/MEPS46793.2019.9395055.
5. Globa, Larysa & Kurdecha, Vasyl & Popenko, Demyd & Bezvuhliak, Maksym & Porolo, Yevgeniy. (2022). Data Collection and Processing Method in the Networks of Industrial IOT. 10.1007/978-3-031-15101-9_11.

УДК 004.01:004.71:004.72:004.032

ПРОБЛЕМИ АУДИТУ ІНФОКОМУНІКАЦІЙНОЇ МЕРЕЖІ ВЕЛИКИХ ПІДПРИЄМСТВ

Ковальська Д.Д., Курдеча В.В.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: darinakovalskaaa@gmail.com

PROBLEMS OF AUDITING THE INFORMATION COMMUNICATION NETWORK OF LARGE ENTERPRISES

Increasing informatization of society leads to the need for effective methods of creating, controlling and auditing information communication networks. The method of auditing the information communication network of large enterprises is an integral part of infrastructure management and its security. It includes the collection and analysis of data on the state of the network, checking its resistance to external threats, testing equipment for resistance to attacks and other important processes.

Аудит як поняття у телекомунікаціях означає збір даних для аналізу та подальшої обробки, в основному, із ціллю удосконалення існуючої мережі. Це невід'ємна частина модернізації та перевірки поточного стану існуючої інфраструктури. Метод аудиту інфокомунікаційної мережі великих підприємств є невід'ємною частиною управління інфраструктурою та її безпекою. Він включає в себе збір та аналіз даних про стан мережі, перевірку її стійкості до зовнішніх загроз, тестування обладнання на стійкість до атак та інші важливі процеси.

Модернізація методів аудиту інфокомунікаційної мережі є необхідною для забезпечення безперебійної роботи великих підприємств. Сучасні технології дозволяють автоматизувати процеси збору та обробки даних, що забезпечує високу достовірність результатів та скорочення часу на проведення аудиту. Крім того, використання програмного забезпечення дозволяє проводити інвентаризацію обладнання автоматично, що зменшує необхідність у фізичному втручанні спеціалістів і зменшує витрати на аудит.

При цьому, модернізація методів аудиту дозволяє підвищити рівень безпеки мережі та забезпечити стійкість до зовнішніх загроз. Таким чином, впровадження нових методів аудиту допоможе підприємствам ефективніше використовувати ресурси та зменшити ризики виникнення проблем в роботі мережі.

Однією з головних проблем, які можуть виникнути при аудиті мережі, є необхідність у великій кількості людських ресурсів та часі для збору та обробки даних про стан мережі. Крім того, традиційні методи аудиту можуть бути неефективними у виявленні нових загроз та уразливостей, що можуть виникати з часом.

Це може бути складним і затратним процесом для компаній, що не мають достатнього досвіду в галузі мережевої безпеки.

Однак, існує ряд нових технологій, які можуть допомогти вирішити ці проблеми. Наприклад, автоматизовані системи моніторингу та виявлення інцидентів можуть значно скоротити час на виявлення та реагування на проблеми в мережі. Штучний інтелект та машинне навчання також можуть бути використані для аналізу великої кількості даних та виявлення нових загроз та уразливостей.

Крім того, зростаюча популярність хмарних технологій та віртуалізації дозволяє компаніям зменшити кількість необхідних фізичних ресурсів та спростити управління мережею.

Використання сучасних технологій та програмного забезпечення може вирішити ці проблеми, дозволяючи автоматизувати процеси збору та обробки даних, а також проведення інвентаризації обладнання. Це забезпечує високу достовірність результатів та скорочення часу на проведення аудиту. Більше того, такий підхід може допомогти виявляти нові загрози та уразливості та вчасно їх усувати, що забезпечить високий рівень безпеки мережі.

Іншою важливою проблемою є зменшення витрат на аудит. Використання програмного забезпечення дозволяє проводити інвентаризацію обладнання автоматично, що зменшує необхідність у фізичному втручанні спеціалістів та зменшує витрати на аудит .Участь у управлінні мережею та її безпекою - регулярне проведення аудиту, який має бути виконаний професіоналами з відповідним досвідом та знаннями. Однак, з огляду на високу складність мереж та збільшення їх обсягу, ручне виконання аудиту стає все складнішим та часозатратним, а також не виключає можливість людської помилки. Тому, використання сучасних технологій та програмного забезпечення є надзвичайно важливим для оптимізації процесу аудиту та забезпечення ефективного управління мережею.

Наприклад, однією зі сучасних технологій, яка може бути використана для аудиту, є технологія "інтернету речей" (Internet of Things, IoT). Вона дозволяє підключати до мережі різні пристрої, які забезпечують збір та передачу даних про стан мережі. За допомогою аналізу цих даних можна виявляти вразливості та загрози, що дозволяє підвищити рівень безпеки мережі та запобігти виникненню проблем у роботі. На рис. 1 представлене реальне застосування програмного забезпечення Netdisco для мережевого аудиту великого виробництва, на рисунку представлений повний перелік усіх мережевих пристроїв та як вони з’єднані один з одним.

Netdisco застосовується для збору інформації щодо активних MAC-адрес із подальшим зберіганням у своїй базі даних. Дані збираються з використанням опитувань SNMP і DNS-запитів, отримання представлення – за допомогою Mason.

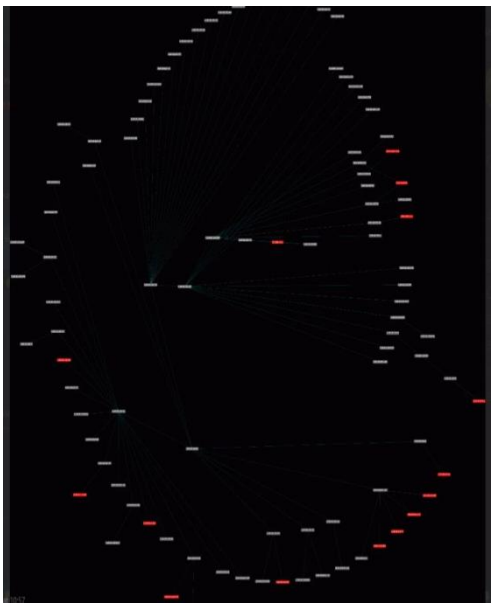


Рис. 2. Результат роботи ПЗ Netdisco.

У загальному, необхідно використовувати нові технології та інструменти для покращення ефективності аудиту мережі та забезпечення мережевої безпеки. Важливо також забезпечити постійне навчання та підвищення кваліфікації спеціалістів, що займаються мережевою безпекою, щоб вони могли ефективно використовувати нові технології та інструменти.

Отже, аналізуючи вище представлену інформацію, можна дійти висновку що спрощення аудиту і перехід від фізичного до аудиту із, у більшій мірі, застосуванням програмного забезпечення є можливим, і, більше того, необхідним.

Модернізація методів аудиту дозволяє ефективніше використовувати ресурси та зменшувати ризики виникнення проблем в роботі мережі. Використання сучасних технологій та програмного забезпечення забезпечує автоматизацію процесів збору та обробки даних, що забезпечує високу достовірність результатів та скорочення часу на проведення аудиту.

Однак, необхідно враховувати важливість постійного моніторингу мережі та вчасного виявлення нових загроз та уразливостей для забезпечення високого рівня безпеки мережі.

Література

1. Гаврилова Л.В., Ян ван Тайнен, Шкуропат О.Г., Манфред ван Кестерен, Герард ван ден Берг, Рудніцька Р.М.,Чорнуцький С.П., Тимохін М.Г., Боровкова Т.В., Любиш-Родченко А.Г., Горбачев С.В.//ПРАКТИЧНА МЕТОДОЛОГІЯ ІТ-АУДИТУ
2. Самойленко В.В. Локальні мережи. Повне керівництво. — К., 2002. — ISBN 966-7140-28-8. Архивна копія от 11 січня 2012 на Wayback Machine.

УДК 519.873

СИСТЕМА МОДЕЛЮВАННЯ ДОСТУПНОСТІ МЕРЕЖЕВИХ ПОСЛУГ

Вішталь Д.М., Любашенко Н.Д.
Факультет прикладної математики КПІ ім. Ігоря Сікорського, Україна
E-mail: ndp1992@bigmir.net

NETWORK SERVICE AVAILABILITY MODELING SYSTEM

Questions of designing of modeling system for calculating probability of network service availability are considered. Characteristics of quality and efficiency of functioning of a network depend on structure of a network and weight parameters of elements

Доступність мережевої послуги – це здатність мережі забезпечити будь-якого користувача зв'язком у будь-який момент часу. Моніторинг цієї характеристики мережі може застосовуватись в процесі експлуатації системи, зміни її елементів. Доступність мереж можна охарактеризувати за допомогою методологій оцінювання [1], таких як блокова діаграма надійності (RBD, Reliability Block Diagram), аналіз дерева відмов (FTA, Fault Tree Analysis) [2], тощо. Типові алгоритми визначення доступності мережі включають метод перерахування станів [3], метод факторизації [4], клітинні автомати [5].

В даній роботі використано стандартну модель мережі - зважений граф.

Для моделювання мережі запропоновано ймовірнісну модель з двома станами – робочий, неробочий - як для окремих елементів, так і для всієї мережі. Стан мережі визначається станом елементів і описується відповідною структурною функцією

$$\varphi(x_1(t), x_2(t), \ldots, x_n(t)) = \begin{cases} 1, \text{ якщо в момент часу } t \text{ система в робочому стані} \\ 0 \text{ в іншому випадку} \end{cases}$$

Якщо $s, t \in Y$ - дві довільні вершини мережі, то стаціонарна ймовірність (s-t) зв'язності мережі $P\left\{\varphi_{s,t}\left(x_1, \ldots, x_n\right) = 1\right\}$ характеризуватиме доступність мережевої послуги.

Формалізація задачі оцінювання стаціонарної ймовірності парної зв'язності базується на ізоморфізмі булевої алгебри функцій властивостей $U_{\Phi} = \langle x_1, x_2, \ldots, x_n; \wedge; \vee; ^{-} \rangle$ і відповідної булевої алгебри класів станів $U_K = \left\langle P\left(B_2^n\right); \cap; \cup; ' \right\rangle$, де $\{x_1, ..., x_n\}$ - утворюючі булевої алгебри функцій, B_2^n - векторний простір станів елементів мережі, потужність $\left|B_2^n\right| = 2^n$, розмірність $\dim\left(B_2^n\right) = n$. Вводяться такі припущення: всі вузли є абсолютно надійними; залежністю випадкових величин часових інтервалів доступності (недоступності) нехтуємо; мережа розглядається як система з повнодоступним відновленням; при заданому режимі інформаційного навантаження на мережу (мала, середня, велика) встановлюється стаціонарний режим; стан мережі відносно $\varphi_{s,t}$ - доступності (недоступності)

визначається станом її елементів при заданому навантаженні мережі; вектор станів однозначно визначає (s-t) зв'язність мережі.

Даний підхід дозволив розробити ефективні алгоритми для програмування обчислень.

Процес функціонування мережі розглядається як дискретно-неперервний випадковий процес блукання по булевій векторній решітці.

Для обчислення ймовірності пропонується спочатку знайти всі найкоротші (s-t) шляхи мережі, мінімальні (s-t) перерізи мережі. Вибране представленння функції зв’язності ортогоналізується для функції $\varphi_{s,t}(x_1,\ldots,x_n)$, поданої в мінімальній диз'юнктивній нормальній формі. Тоді $\varphi_{s,t}(x_1,\ldots,x_n) = f_1 \vee \ldots \vee f_m = f_1 + \overline{f}_1 f_2 + \overline{f}_1 \overline{f}_2 f_3 + \ldots + \overline{f}_1 \ldots \overline{f}_{m-1} f_m$, де f_i - i-й (s-t) шлях мережі; m - кількість (s-t) шляхів мережі.

На основі отриманого представлення конструюється формула для проведення обчислень на наступному етапі моделювання.

Приклад формули, отриманої для визначення ймовірності доступності мережі (рис. 1) між вузлами Y1 та Y6, наведено на рис. 2, де p_i - коефіцієнт стаціонарної готовності i-го каналу мережі; $q_i = 1 - p_i$.

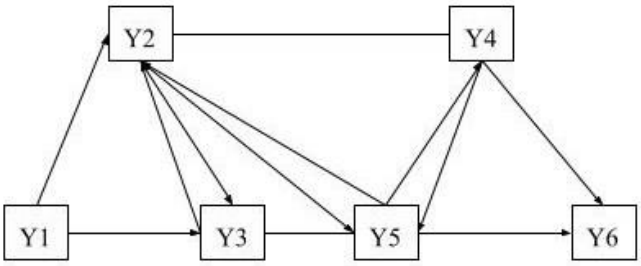


Рис.1. Граф мережі.

$$
\begin{aligned}
P_{s,t} = {} & 1 - q_1 q_2 - (1 - q_1 q_2) q_{11} q_{12} - p_2 (1 - q_{11} q_{12}) q_1 q_3 q_8 - (1 - q_{11} q_{12})(1 - q_1 q_2 - p_2 q_1 q_3) q_5 q_6 q_8 - \\
& - p_{11} (1 - q_1 q_2 - p_2 q_1 q_3 q_8 - (1 - q_1 q_2 - p_2 q_1 q_3) q_6 q_8) q_5 q_9 q_{12} - \\
& - p_1 p_8 (1 - q_{11} q_{12} - p_{11} q_9 q_{12}) q_2 q_4 q_5 q_6 - p_5 p_{12} (1 - q_1 q_2 - p_2 q_1 q_3) q_6 q_8 q_{10} q_{11} - \\
& - p_1 p_5 p_8 p_{12} q_2 q_4 q_6 q_{10} q_{11} - p_2 p_5 p_8 p_{11} q_1 q_3 q_7 q_9 q_{12}.
\end{aligned}
$$

Рис.2. Приклад теоретичної формули.

Оскільки при збільшенні кількості вершин та ребер графа формула виглядатиме громіздко, а також враховуючи, що значення p_i та q_i не перевищують одиницю, пропонується до початку обчислень перетворити рядок теоретичної формули до робочого вигляду, не втративши задану точність обчислень. Зокрема, можна скоротити кількість доданків, які містять малі множники. Наприклад, якщо у наведеній формулі оцінити доданки, які містять п'ять множників q, то, замінивши p на 1, а q на 0.5, отримаємо грубу оцінку результату, що не перевищуватиме 0.032. Аналогічно, в доданках з шістьма множниками q, результат не перевищуватиме 0.016, у виразах з сімома множниками q, результат не

перевищуватиме 0.008.

Якщо користувача влаштовує оцінка з точністю до десятих, можна використати наступну робочу формулу:

$$P_{s,t} = 1 - q_1 q_2 - (1 - q_1 q_2) q_{11} q_{12} - p_2 q_1 q_3 q_8 - q_5 q_6 q_8 - p_{11} q_5 q_9 q_{12} - p_1 p_8 q_2 q_4 q_5 q_6 - p_5 p_{12} q_6 q_8 q_{10} q_{11}.$$

Для реалізації запропонованої моделі оцінки доступності мережевої послуги, алгоритмів побудови формули обчислення ймовірності доступності розроблено проект відповідної системи (рис. 3). Структура мережі задається матрицею суміжності.

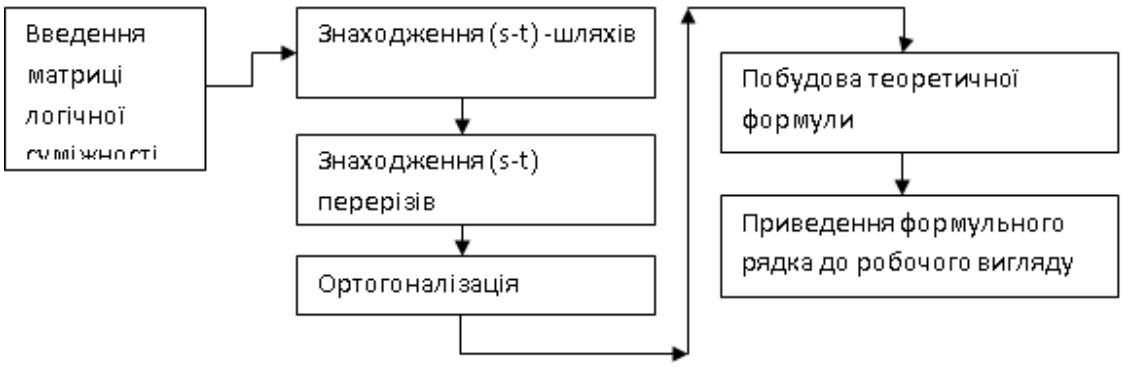


Рис.3. Структура системи оцінювання доступності мережевої послуги.

Запропонований проект системи після реалізації всіх складових забезпечить:

- розв'язок задач синтезу мереж із заданими властивостями;
- оцінку середнього стаціонарного часу перебування мережі у стані доступності;
- оцінку важливості елементів, тобто рівень впливу коефіцієнта готовності елемента на коефіцієнт готовності мережі при наданні мережевої послуги.

Література

1. Zio E. Reliability engineering: Old problems and new challenges. Reliability Engineering and System Safety 2008; 6: 128-133, DOI:10.1016/j.ress.2008.06.002
2. Volkanovski A, Cepin M, Mavko B. Application of the fault tree analysis for assessment of power system reliability. Reliability Engineering & System Safety 2009; 94: 1116–1127, DOI:10.1016/j.ress.2009.01.004
3. Shier DR. Network Reliability and Algebraic Structures. Oxford: Clarendon Press; 1991.
4. Wood RK. Factoring Algorithms for Computing K-Terminal Network Reliability. IEEE Transactions on Reliability 1986; 35: 269-278, DOI:10.1109/TR.1986.4335431
5. Rocco CM, Zio E. Solving Advanced Network Reliability Problems by Means of Cellular Automata and Monte Carlo Sampling. Reliability Engineering and System Safety 2005; 89: 219-226, DOI:10.1016/j.ress.2004.08.025.

УДК 621.3:519.2

ДЕТЕКТОР СТОХАСТИЧНИХ СИГНАЛІВ

Бугайов М.В.
Житомирський військовий інститут імені С.П. Корольова, Україна
E-mail: karunen@ukr.net

STOCHASTIC SIGNALS DETECTOR

Robust for signal structure and noise power uncertainty detector for stochastic signal detection and time parameters estimation was proposed. For threshold calculation in given frequency channel detector uses energy estimates of received signal.

Через стрімкий розвиток радіосистем із використанням технології програмно-визначеного радіо з'явилася можливість формувати сигнали практично будь-якої форми [1-2]. Даний факт призводить до ускладнення радіоелектронної обстановки і стимулює теоретичні та практичні дослідження щодо удосконалення методів та алгоритмів виявлення стохастичних сигналів. При невідомій структурі сигналу найбільш доцільно розробляти модифікації енергетичного детектора. Такий підхід забезпечить швидке оцінювання зайнятості частотного каналу для систем когнітивного радіо [3].

Рішення про виявлення сигналу в енергетичному детекторі може прийматися шляхом порівняння кожного відліка енергії прийнятого комплексного сигналу з порогом, значення якого визначається необхідною ймовірністю хибної тривоги P_F. Значення енергії E відліка комплексної суміші x сигналу s та шуму ξ будемо розраховувати за таким виразом:

$$E = x_I^2 + x_Q^2, \tag{1}$$

де $x_I = s_I + \xi_I$ – синфазна складова;

$x_Q = s_Q + \xi_Q$ – квадратурна складова.

Значення E для шуму підпорядковане експоненціальному розподілу щільності ймовірностей (РЩЙ). Тоді поріг для значення ймовірності хибної тривоги P_F розраховується за таким виразом:

$$\gamma = -\sigma_\xi^2 \, ln\left(P_F\right), \tag{2}$$

де $\sigma_\xi = \sqrt{\sigma_{\xi_I}^2 + \sigma_{\xi_Q}^2} = \sqrt{2}\sigma_{\xi_I} = \sqrt{2}\sigma_{\xi_Q}$ – середньоквадратичне відхилення шуму (СКВ). Причому значення σ_ξ перед початком спостережень невідоме і потребує оцінювання.

У даній роботі рішення про виявлення сигналу запропоновано приймати не за кожним відліком E, а за енергією, що міститься в L відліках відповідно до такого виразу:

$$E_L = \sum_{i=1}^{L}\left(x_I^2(i) + x_Q^2(i)\right). \tag{3}$$

Вибіркові значення енергії E_L будуть підпорядковані гамма-розподілу [4]. Значення порогу γ для E_L можна розрахувати як квантиль гамма-

розподілу рівня $p = 1 - P_F$. Для цього використаємо апроксимацію квантиля гамма-розподілу із використанням розподілу хі-квадрат χ^2:

$$\gamma_p = \chi_p^2\left(2\left(L+1\right)\right), \tag{4}$$

де $\chi_p^2\left(2\left(L+1\right)\right)$ – значення квантиля рівня p для розподілу χ^2 з $K = 2\left(L+1\right)$ ступенями свободи.

Із використанням апроксимації Вілсона-Хілферті квантилів розподілу χ^2 [5] значення порогу γ можна розрахувати за таким виразом:

$$\gamma = C\left(1 - \frac{2}{9K} + u\sqrt{\frac{2}{9K}}\right)^3, \tag{5}$$

де C – уточнене значення енергії E_L і

$$u = \frac{1{,}24 + 0{,}85H^{0{,}657}}{1 + 0{,}0001H^{-3} + \dfrac{2{,}38}{H}},\ H = -0{,}96\,ln\left(\frac{P_F}{1 - P_F}\right). \tag{6}$$

Значення C розраховується як середнє арифметичне значень енергії E_L для тих інтервалів сигналу, де поріг не перевищено. Там де поріг перевищується значення C не уточнюється.

При аналізі виділеного частотного каналу в момент початку спостереження сигнал у досліджуваному частотному каналі може бути відсутній або присутній. Оскільки рівень шуму невідомий, тому його значення замінюється оцінкою значення енергії в каналі. В такому разі для другого випадку ми зможемо виявити лише закінчення сигналу за ознакою зменшення рівня енергії в каналі. Для великих L (більше 30) РЩЙ значень E_L можна наближено вважати нормальним. Тоді за ознаку закінчення сигналу можна прийняти зменшення СКВ енергії E_L у 6 разів. Це з ймовірністю близько 0,997 свідчитиме про те, що різка зміна енергії в каналі пов’язана саме із закінченням сигналу.

На рис. 1 наведено результати оброблення прийнятих відліків у частотному каналі для випадків, коли сигнал відсутній (а) та присутній (б).

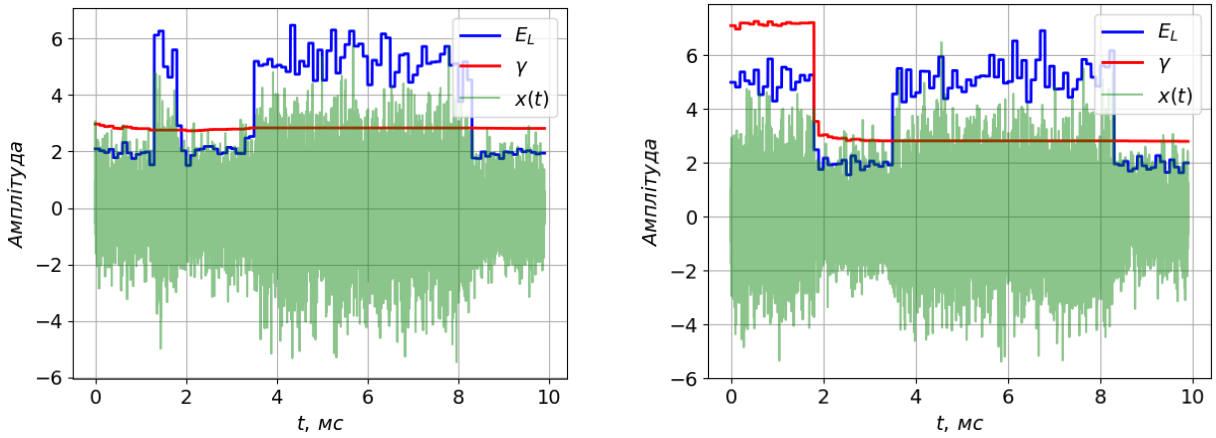


Рис. 1. Оброблення прийнятих відліків у частотному каналі для випадку відсутнього (а) та присутнього (б) на момент початку спостереження сигналу.

Значення ймовірності хибної тривоги складало при цьому $P_F = 10^{-4}$, довжина інтервалу інтегрування $L = 100$, частота дискретизації становила 10 МГц, відношення сигнал-шум складало 2 дБ. Як сигнал використано імпульси з прямокутною обвідною, що заповнені білим гауссівським шумом. З даних рисунків видно, що на початковому етапі роботи детектора значення порогу коливається. Причому дані коливання зменшуються при збільшенні L. Проте вибір великих значень L призведе до погіршення точності оцінювання часу початку та закінчення сигналу.

На рис. 2 наведено криві виявлення для розробленого детектора, що використовує статистику E_L для порівняння з порогом (5) та статистику E для порівняння з порогом (2). Довжина вікна інтегрування при цьому складала 100, а ймовірність хибної тривоги для обох детекторів була задана на рівні 10^{-4}. Як бачимо, розроблений детектор потребує приблизно на 5 дБ меншого відношення сигнал-шум для забезпечення такої ж ймовірності правильного виявлення P_D що і детектор на основі статистки E. Причому для роботи останнього потужність шуму повинна бути відомою. Уточнення розрахованого значення порогу за відсутності сигналу проводити рекомендовано не постійно, а протягом деякого інтервалу часу. Після чого накопичене значення скидати і уточнення проводити заново.

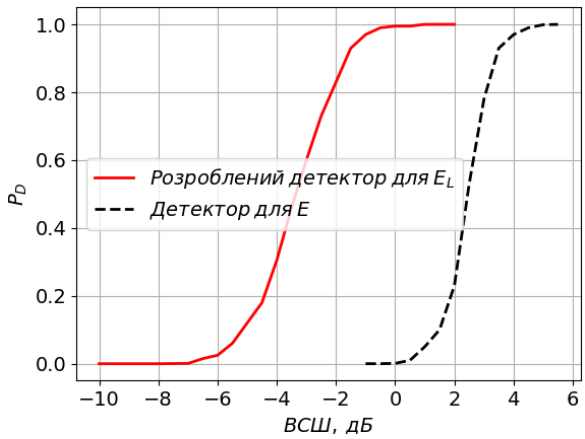


Рис. 2. Криві виявлення для детекторів при $P_F = 10^{-4}$ і $L = 100$

Запропонований детектор дозволяє виявляти та визначати часові межі стохастичних сигналів на фоні невідомого і змінного значення потужності шуму. Детектор може бути реалізований в системах когнітивного радіо, автоматичних комплексах радіомоніторингу та інших радіосистемах, де необхідно проводити швидке оцінювання зайнятості частотних каналів. Перспективи подальших досліджень в даному напрямку доцільно зосередити в розробленні алгоритмів уточнення часових меж виявлених сигналів.

Література

1. Liang Y.-C. Dynamic Spectrum Management. From Cognitive Radio to Blockchain and Artificial Intelligence. Springer, 2020. 180 p.
2. Elmasry F. G. Dynamic Spectrum Access Decisions. Local, Distributed, Centralized, and Hybrid Designs. JohnWiley & Sons Ltd., 2021. 728 p.
3. Captain K. M., Joshi M. V. Spectrum Sensing for Cognitive Radio. Fundamentals and Applications. CRC Press. 2022. 256 p.
4. Kay S. M. Fundamentals of Statistical Signal Processing: Practical Algorithm Development. New York: Prentice Hall, 2013. 475 p.
5. Zar J. H. Approximations for the Percentage Points of the Chi-Squared Distribution. Journal of the Royal Statistical Society. Series C (Applied Statistics). Vol. 27, No. 3, 1978. pp. 280-290.

UDC 621.372.543

MICROWAVE DIRECTIONAL FILTERS

Zhivkov A.P., Shevtsov K.O., Kamarali R.V.,
Krylach O.F., Stepanenko V.M.
National Technical University of Ukraine
“ Igor Sikorsky Kyiv Polytechnic Institute ”
E-mail: shewtsov.kostya@gmail.com,
a.zhivkov@kpi.ua , r.kamarali@kpi.ua

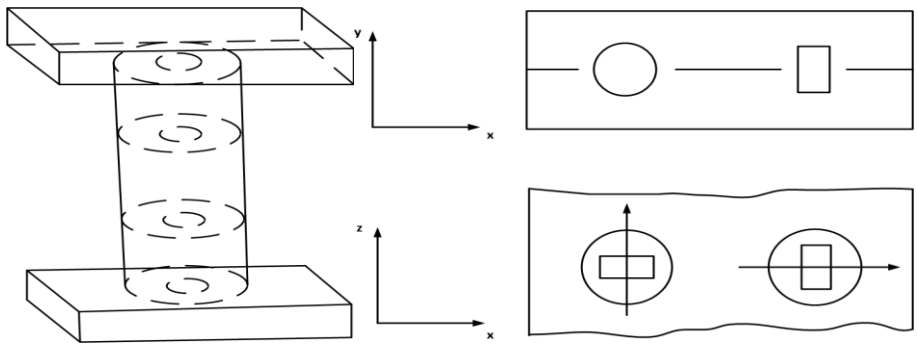
МІКРОХВИЛЬОВІ СПРЯМОВАНІ ФІЛЬТРИ

У статті описано конструкцію та властивості спрямованих фільтрів на основі кругових резонаторів і діелектричних резонаторів. Змодельовані метаматеріальні властивості спрямованих фільтрів у сучасній мікрохвильовій технології.

This article describes construction and properties of directional filters based on circular resonators and dielectric resonators. Simulated metamaterial properties of directional filters in modern microwave technology.

In modern microwave technology, directional filters - so-called directional filters - with directional properties are widely used, which were considered in [1]. Interest in them has re-emerged because these devices have some "metamaterial" properties.

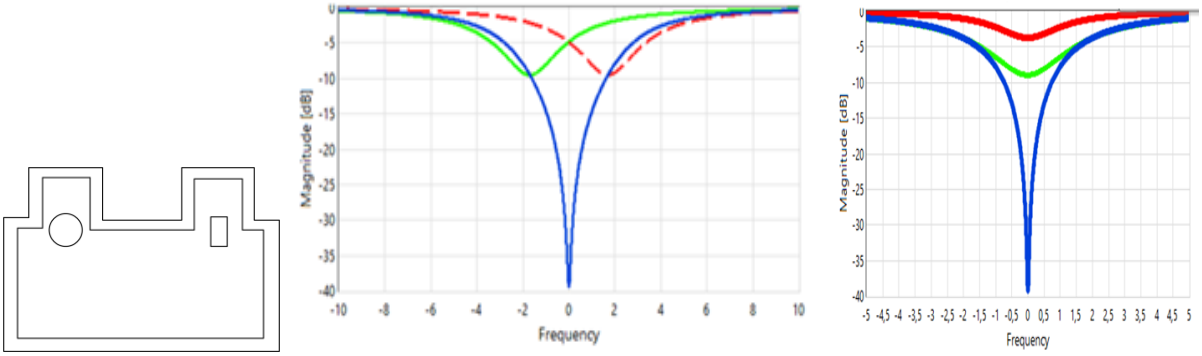
Fig. 1 (a) shows the waveguide structure of a directional filter from [2], this filter consisted of circular resonators excited by holes located in the circular polarization region of rectangular waveguides. A modernized version of such directional filter based on dielectric resonators (DR) in the circular polarization regions of rectangular waveguides was patented in 1987 [3], and its characteristics as well as the characteristics of bandpass (BPF) and rejector filters (RF) were published in [4], the structure of the specified filter is shown in Fig.1 (b)



(a) (b)

Fig. 1. (a) The waveguide structure of a directional filter;
(b) bandpass and rejector filters.

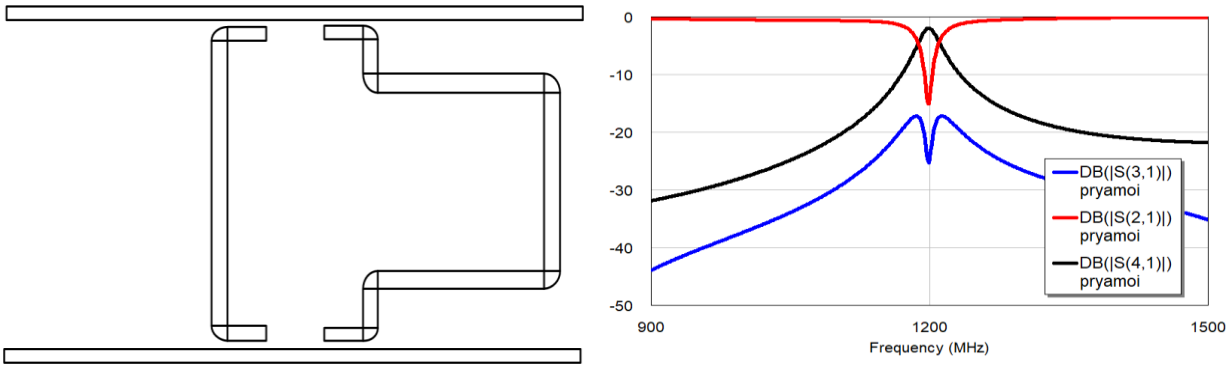
The RF, which consists of only one waveguide with two DRs in the circular polarization region Fig.2 (a) as described in [3], demonstrates a characteristic in the form of a "degenerate" oscillation, obtained as the interference of oscillations from individual resonators [4], which is commonly referenced as "Fano resonances" in modern literature [5].



(a) (b) (c)

Fig. 2. (a) The RF, which consists of only one waveguide with two DRs in the circular polarization region; (b), (c) modeled filter characteristics.

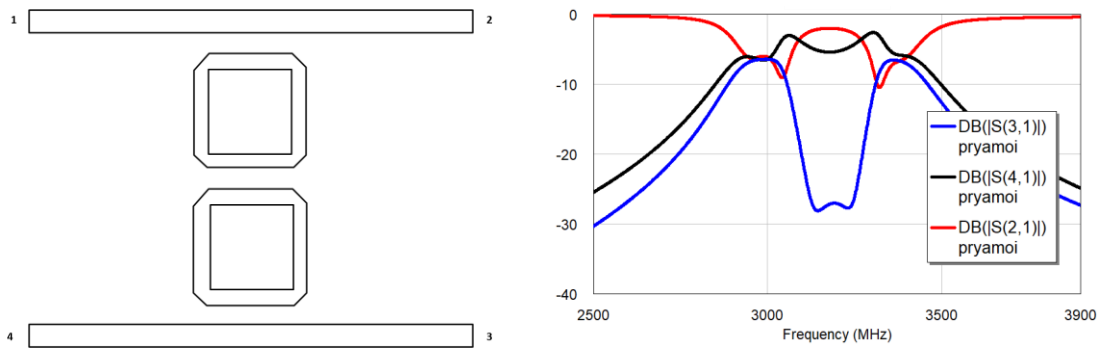
The filter shown in fig. 3 a) is formed by two microstrip resonators - "half-wave" and "wave" and when choosing the distance between the resonators so that at output 3 their oscillations are in phase, and at output 4 - in antiphase, we observe its characteristics presented in Fig. 3 b).



(a) (b)

Fig. 3. (a) filter formed by two microstrip resonators - "half-wave" and "wave" ;(b) simulated filter characteristics.

The red curve in fig. 3 b) similarly to the RF characteristic, demonstrates that at the resonance frequency the energy is "taken" from the line connecting outputs 1 and 2 to output 3.



(a) (b)

Fig. 4. (a) filter formed by interconnected resonators;
(b) simulated characteristics of the specified filter.

In a filter formed by interconnected resonators Fig. 4 (a), the energy in the region of the center frequency is distributed somewhat differently - it is divided between outputs 2 and 3 but is not supplied to output Fig. 4 (b).

Conclusion. design and properties of directional filters based on circular resonators and dielectric resonators were described. These filters have "metamaterial" properties and are widely used in modern microwave technology.

The characteristics of bandpass and rejector filters, as well as the characteristics of the filters formed by two microstrip resonators and resonators connected to each other, are given. It is important to emphasize the phenomena of "Fano resonances" observed in these filters, which are arise as the interference of oscillations from individual resonators.

References

1. Microwave Filters, Impedance-Matching Networks, and Coupling Structures, by George L. Matthaei, Leo Young, and E. M. T. Jones. Published (1964) by McGraw-Hill Book Co. Inc.
2. Coale, F. S. (1956). A Traveling-Wave Directional Filter. IEEE Transactions on Microwave Theory and Techniques, 4(4), 256–260. doi:10.1109/tmtt.1956.1125073
3. USSR Inventor's certificate 1417082.
4. M. E. Ilchenko and A. P. Zhivkov, “UHF devices based on several dielectric-cavity mode types”, Radioelectronics and Communications Systems (English translation of Izvestiya Vysshikh Uchebnykh Zavedenii Radioelektronika), 1989, 32(5), pp. 54–57
5. Kamenetskii, E., Sadreev, A., & Miroshnichenko, A. (Eds.). (2018). Fano Resonances in Optics and Microwaves. Springer.

УДК 004.8

ЗАСТОСУВАННЯ МЕТОДІВ НЕЧІТКОЇ ЛОГІКИ ДЛЯ ПРОГНОЗУВАННЯ ДОРОЖНЬОГО ТРАФІКУ

Цуканов С.О., Глоба Л.С.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: *sergeyidus@gmail.com*

APPLICATION OF Fuzzy LOGIC METHODS FOR ROAD TRAFFIC FORECASTING

The paper considers the method of developing fuzzy logical rules for predicting traffic congestion in real time. The construction of a set of fuzzy logical rules for predicting traffic congestion is described step by step.

Затори на дорогах у великих містах стають гострою проблемою, що зачіпає кошти для існування людей, а також соціальний та економічний розвиток. Значне зниження продуктивності транспортної системи призводить до збільшення часу подорожі, що ускладнює переміщення людей і товарів, що в свою чергу веде до зменшення торгівлі та економічної активності в містах. Фактори, пов'язані із заторами в США, становлять понад 305 мільярдів доларів прямих та непрямих витрат лише у 2017 році, що на 10 мільярдів доларів більше, ніж у 2016 році, що зумовлено збільшенням вартості автомобілів, а не збільшенням заторів як таких. Прямі витрати включають вартість палива і час, витрачений в пробках, в той час як непрямі витрати включають збільшення цін для домогосподарств через те, що вантажні автомобілі стоять в заторах.

Необхідність прогнозування дорожньо-транспортного руху для поліпшення логістичної ситуації, особливо це стосується мегаполісів, обумовлюється тим, що це дозволяє попередити можливі затори, які можуть виникнути на конкретній ділянці транспортної мережі. Це дозволяє

Виходячи з перерахованих вище факторів, регулювання пропускної спроможності доріг набуває особливого значення. Для чого На сьогоднішній день широко застосовуються системи Інтернет речей (IoT). Прогнозування заторів на дорогах може допомогти керувати транспортною інфраструктурою та запобігати їх виникненню. Це може включати зміну світлофорних режимів, перенаправлення трафіку або попередження водіїв про можливі затримки.

В роботі пропонується підхід до регулювання дорожньо-транспортного руху за допомогою системи IoT, побудованої на основі статистичних даних бази нечітких знань, що дозволить виявити закономірності завантаженості трафіку у різні моменти часу на різних ділянках. Основна перевага полягає в тому, що використання нечіткої бази знань не потребує великих обчислювальних ресурсів, що дає можливість реалізовувати процес регулювання дорожньо-транспортного руху в системі IoT безпосередньо на дорозі в оперативній обстановці.

Існують різні математичні методи та технології для прогнозування пробок на дорогах, включаючи:

Використання даних про рух транспорту: на основі даних, які отримуються від систем моніторингу трафіку, можна створювати прогнози про потік транспорту на

певних ділянках доріг. Такі дані можна отримати, наприклад, за допомогою GPS-моніторів в автомобілях.

Аналіз статистичних даних: аналіз історичних даних про рух транспорту на певних ділянках доріг може допомогти передбачити майбутні тенденції та події, включаючи можливі затори.

Використання математичних моделей: такі моделі можуть бути використані для прогнозування трафіку на дорогах, використовуючи дані про рух транспорту, погодні умови та інші фактори. Наприклад, моделювання потоку транспорту може показати, як зміна одного фактору, такого як час світлофорних сигналів може вплинути на трафік.

Алгоритми машинного навчання можуть бути використані для аналізу даних про рух транспорту та прогнозування майбутніх ситуацій в системі IoT дорожньо-транспортного руху. Наприклад, нейронні мережі можуть бути навчені розпізнавати патерни руху транспорту та робити прогнози на основі цих даних. Але алгоритми машинного навчання мають велику обчислювальну складність, що ускладнює їх застосування в системі IoT дорожньо-транспортного руху.

Для прогнозування дорожнього трафіку пропонується застосовувати методи нечіткої логіки для побудови нечітких логічних правил, які будуть описувати завантаженість трафіку в залежності від його параметрів та які дозволять знизити високу обчислювальну складність під час прийняття рішень.

Запропонований в роботі алгоритм працює тільки з числовими даними.

Вхідною інформацією для формування нечітких логічних правил є набір даних у вигляді таблиці в якому наявні наступні стовпці:

Smean - середня швидкість;

Sstddev - середньо-квадратичне відхилення швидкості;

t- час виміру швидкості;

Smaxv - максимальна швидкість;

l - довжина маршруту;

Q – завантаженість.

Далі проводиться нормалізація вхідних даних *Smean, S_stddev, t, Smaxv, l, Q,* а саме перетворення числових даних таким чином, щоб усі вони лежали в межах між 0 та 1.

Далі для отримання нечітких логічних правил з нормалізованих даних застосовано алгоритм кластеризації Kmeans, сутність якого полягає в наступному.

Крок 1. Визначається кількість кластерів, в нашому випадку їх буде три.

Крок 2. З векторів вхідної інформації випадковим чином, у вхідних даних обираються початкові центри кластерів.

Крок 3. Для кожного з векторів вхідної інформації обчислюються евклідові відстані до центрів кластерів.

Кожен вектор приписується до того кластера для якого евклідова відстань до нього буде найменшою.

Крок 4. Наступним кроком буде перерахунок положення центрів кластерів.

Новий центр кластера буде дорівнювати середньому арифметичному значенню векторів цього кластера.

Критерій зупинки. Алгоритм кластеризації припиняє свою роботу коли центри сформованих кластерів перестають змінюватися.

Слід зазначити, що можливо використання різноманітних модифікацій алгоритму Kmeans, або тих алгоритмів кластеризації, в яких кількість кластерів

можна обрати заздалегідь.

Далі будуємо функції приналежності для кожного з компонентів векторів вхідної інформації *S_mean,S_stddev,t,Smaxv,l,Q.*

В якості функції приналежності було обрано Гауссову функцію приналежності.

Для того щоб побудувати функції приналежності для кожної компоненти вхідної інформації необхідно взяти відповідні компоненти з центрів сформованих кластерів це будуть математичне очікування функції приналежності.

Для знаходження середньоквадратичного відхилення скористаємося формулою:

$$\frac{m_{xi} - m_{x(i+1)}}{3N_x}$$

де m_{xi} – центр кластера, $m_{x(i+1)}$ – центр найближчого кластера, N_x – кількість кластерів.

За кожною функцією приналежності закріплено задане лінгвістичне значення. Наприклад для функції з мінімальним математичним очікуванням це значення ‘мало’, а з найбільшим - ‘багато’. Лінгвістичне значення для кожної функції приналежності задається заздалегідь на етапі, коли обирається кількість кластерів.

Далі відбувається перехід від числових значень до лінгвістичних. Цей перехід відбувається наступним чином: для кожної компоненти кожного вектору вхідної інформації обраховується значення функцій приналежності, числове значення набуде лінгвістичного значення тієї функції приналежності для якої значення функції від цього значення буде найбільшим.

Після цього кожен рядок можна представити у вигляді нечіткого логічного правила вигляду:

Якщо S_mean = mid and S_stddev = mid and ... and l = high then Q = low,

Останньою операцією буде видалення конфліктів та дублікатів. Конфліктом, в даному випадку, називається ситуація, коли у наборі нечітких логічних правил існують правила, в яких всі змінні, окрім прогнозованої мають однакові значення, а прогнозована змінна відрізняється. Тоді для видалення конфлікту необхідно:

1. Підрахувати кількість входжень для кожного такого правила
2. Видалити те правило кількість входжень якого менша.

Усунення дублікатів собою являє собою видалення з набору нечітких логічних правил тих входжень, що повторюються. Це робиться для того щоб кожне нечітке логічне правило не повторювалося.

В результаті роботи методу отримаємо набір нечітких логічних правил. За побудованими нечіткими правилами можна прогнозувати завантаженість дорожнього трафіку. Крім того даний метод не потребує великого обсягу обчислювальних ресурсів для прогнозування завантаженості доріг в рамках системи IoT.

Література

1. Глоба Л.С., Бугаєнко Ю.М., Ляшенко А.В., Гребініченко М.В. Analysis of clustering algorithms for use in the universal data processing system // Міжнародна науково-технічна конференція OSTIS 2020 – С. 101–104.
2. Zgurovsky M. The Cluster Analysis in Big Data Mining / M. Zgurovsky, Y. Zaychenko // Big Data: Conceptual Analysis and Applications / M. Zgurovsky, Y. Zaychenko.. – С. 1–42.

УДК 621.382

АНАЛІЗ ПІДХОДІВ ДО КЛАСТЕРИЗАЦІЇ В БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ

Насвіт Ю.О.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: nasvit17@gmail.com

ANALYSIS OF APPROACHES TO CLUSTERIZATION IN WIRELESS SENSOR NETWORKS

This article describes that clustering is an important area of research. Clustering is the most well-known method of topology management in WSN, grouping nodes to manage them and / or performing various tasks in a distributed way. This document contains information about the phase of clustering: methods of creating clusters.

Управління топологією є однією з головних проблем при проектуванні комп’ютерних мереж, особливо в мережах ad-hoc, оскільки кількість вузлів значно висока, а мережева інфраструктура ненадійна [1]. У техніках управління топологією в мережах ad-hoc визначення можливих сусідів для встановлення з'єднань і розпізнавання найкращих сусідів для поетапної передачі даних мають вирішальне значення для покращення масштабованості, споживання ресурсів, надійності тощо. Кластеризація — це тип методів управління топологією, які можуть групувати вузли для підвищення ефективності мережі шляхом керування ресурсами та чергування відповідальності між вузлами для забезпечення справедливості. Кожен кластер складається з певної кількості членів і має один або кілька каналів для керування учасниками, а також для об’єднання, обробки, передачі та керування даними учасників. Нарешті, кожна мережа має одну або кілька базових станцій (BS), які можна використовувати як шлюзи або локальні вузли обробки даних. Базові станції отримують дані від каналів прямо або опосередковано через вузли між каналом і BS, які називаються вузлами-посередниками. Існує кілька етапів створення кластерів та забезпечення зв’язку між членами та BS, які пояснюються нижче.

Фази кластеризації. Як правило, кластеризація включає дві основні фази: групування вузлів і розподіл обов’язків. Групування зазвичай базується

на діаграмах Вороного, але також може бути не-Вороного, як ланцюг або спектр. У структурі Вороного 2D або 3D мережеве середовище поділено на кілька (нерівних) секцій, які називаються кластерами. Кожен кластер має деякі вузли і взаємодіє з іншими кластерами через канали або шлюзи. У ланцюгових структурах вузли в кластері з'єднуються один з одним для досягнення каналів. Іншими словами, кожен вузол має лише два з'єднання з сусідами по ланцюжку для досягнення каналів. У структурі спектра кути вузлів до BS так само важливі, як і відстань до BS. Кути вузлів, як правило, фіксуються методом розгортки сканування (Scanning Sweep) [2]. Кластери створюються на основі різних кутів і відстаней. На рис. 1 показані різні структури кластеризації та їх порівняння. Як у спектрі, так і в ланцюжкових структурах можна виконувати розшаровування, що реалізує багатосктрибкову передачу даних і покращує ефективність мережі, особливо з точки зору споживання ресурсів. Непрямий зв'язок між джерелом і призначенням зменшує споживання енергії, перериваючи довгий шлях від вузла до каналу на більш короткі маршрути, які називаються внутрішньокластерною маршрутизацією. Однак використання цього методу маршрутизації може викликати проблеми з QoS (Quality of Service), наприклад збільшення затримки. Подібно до з'єднання між каналами та BS, вузли в кластерах можуть підключатися до своїх каналів прямо або опосередковано через інших членів кластера.

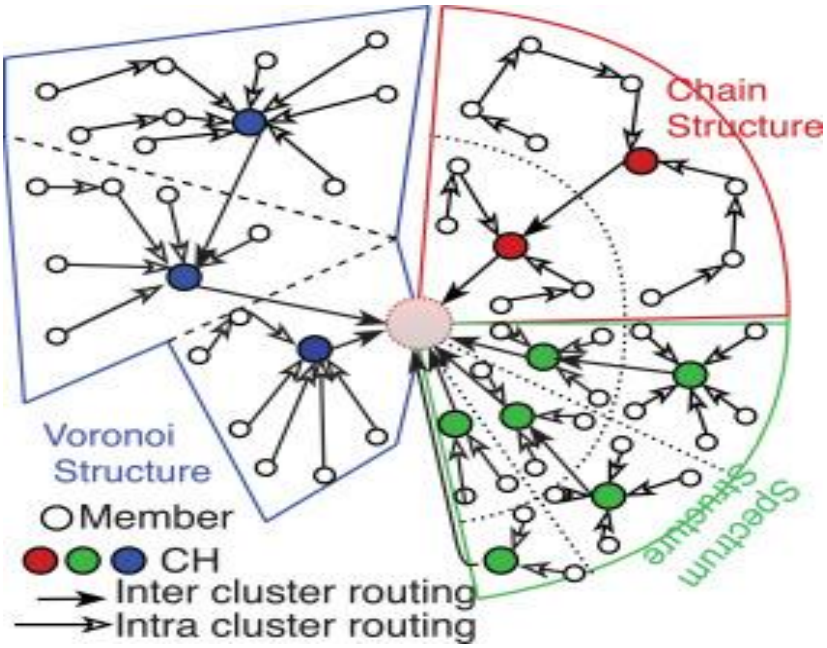


Рис.1. Різні структури методів кластеризації [5].

Методи створення кластерів: Існує два методи створення кластерів у мережі:

- Визначення кластерів шляхом групування вузлів та вибору одного або кількох вузлів як каналів кластера: Групування вузлів може базуватися на різних параметрах, головним чином на фізичній близькості. Крім того, збалансовані кластери з точки зору розміру кластера, кількості вузлів або навантаження мережі можна використовувати як інші параметри для групування вузлів і створення кластерів. Більше того, параметри високого рівня можна використовувати для групування, наприклад, схожість послуг у програмах, які спільно використовують одну мережу, алгоритми збору та об'єднання даних, а також підтримують різні параметри QoS.

- Визначення каналів і запрошення інших вузлів приєднатися до сусіднього каналу: цей метод заснований на таких параметрах, як відстань до каналу і/або відстань каналу від каналу до BS, схожість програм, що працюють на учасників для злиття даних, або запитуваний хостинг послуга(и) головного кластеру.

Література

1. M. Younis, et al. Topology management techniques for tolerating node failures in wireless sensor networks: a survey Comput. Networks, 58 (2014), pp. 254-283
2. H. Le, et al. S-Web: An efficient and self-organizing wireless sensor network model // Proceedings of the International Conference on Network-Based Information Systems, springer (2008), pp. 179-188.
3. Z. Zhang, et al. Energy-efficient multihop polling in clusters of two-layered heterogeneous sensor networks IEEE Trans. Comput., 57 (2) (2008), pp. 231-245
4. W.R. Heinzelman, *et al.* Energy-efficient communication protocol for wireless microsensor networks Proceedings of the Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, IEEE (2000), pp. 1-10
5. https://www.sciencedirect.com/science/article/pii/S1389128620303121#bib0027

УДК 621.369

ВИЗНАЧЕННЯ КООРДИНАТ НАЗЕМНИХ РУХОМИХ ОБ'ЄКТІВ ЗА ДОПОМОГОЮ ГРУПИ БПЛА

Якорнов Є.А., Цуканов О.Ф.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: yakornovits@gmail.com

DETERMINATION OF THE COORDINATES OF GROUND OBJECTS USING THE UAV GROUP

A brief analysis of the methods of determining the coordinates of moving ground objects using a group of UAVs, namely pseudo-range-finding, difference-range-finding and direction-finding methods by a group of 3 or 4 UAVs, was conducted. It is proposed to use the direction-finding method, which allows reducing the number of UAVs to two.

В умовах ведення Україною оборонних, контрнаступальних та наступальних операцій однієї з пріоритетних задач є визначення координат наземних, в першу чергу, рухомих об'єктів в реальному масштабі часу. На теперішний час, вказана задача вирішується за допомогою застосування розвідувальних БПЛА, які мають можливість надавати візуальну інформацію по визначеним цілям.

Розвідувальні БПЛА, мають великий час роботи в повітрі, а це означає їх відносно великі розміри, а значить і більшу ефективну поверхню розсівання, та значний обсяг апаратури, що приводить до їх високої вартості та потребують значний час виробництва. Також, такі БПЛА потребують спеціальні ділянки для базування та зльоту і є першочерговими для знищення цілями ППО противника.

Сучасні тенденції розвитку БПЛА воєнного призначення це зниження вартості, особливо для дронів-камікадзе та підвищення автономності для вирішення задач розвідки. За таких умов вирішення питання застосування малогабаритних БПЛА, які мають на борту мінімальний обсяг апаратури для ведення розвідки, а саме координат наземних рухомих об'єктів противника (цілей) з високою точністю, є актуальною задачею.

Розглянемо методи визначення координат наземних цілей.

1. За допомогою електронних карт. Координати цілей визначається телевізійною камерою БПЛА, а координати визначаються на пункті керування БПЛА за допомогою електронної карти місцевості (система Байрактар). Знищення одного такого БПЛА, приведе до неможливості виконання задачі ведення розвідки.

2. Для підвищення живучості БПЛА (стійкості до вогневого ураження) слід застосовувати групу з трьох або більш БПЛА, що дозволяє визначати координати наземних рухомих цілей без застосування електронних карт.

На даний час, така задача може бути розв’язана [1] за допомогою групи з трьох БПЛА із застосуванням далекомірних методів, далекомірного або різницево-далекомірного, та пеленгаційного за допомогою чотирьох БПЛА. Наприклад, розглянутий в [2] псевдо далекомірний метод полягає в тому що, за допомогою лазерного далекоміра послідовно з трьох точок здійснюється вимірювання відстані до цілі яка розташована на землі. Координати БПЛА визначаються за допомогою системи GPS в реальному масштабі часу, а координати цілі на землі, після виміру дальності з трьох точок. Недоліком цього псевдо далекомірного методу є відсутність можливості визначення дальності лазерним далекоміром, що унеможливлює його застосування.

Тому, для визначення координат наземних рухомих цілей пропонується застосовувати групу БПЛА із застосуванням далекомірного, або разностно – далекомірного метода.

В разі застосування далекомірного методу рис. 1а. пропонується використовувати групу з трьох БПЛА. Для використання різницево-далекомірного методу, групи з чотирьох БПЛА рис.1(b,c).

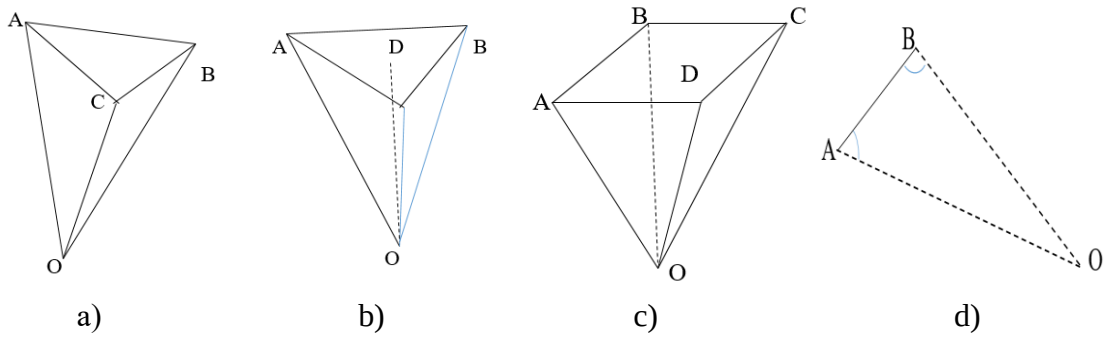


Рис.1. a) далекомірний метод; b) різницево-далекомірний метод; c) пеленгаційний метод 1; d) пеленгаційний метод 2.

Нехай три БПЛА розташовані в точках рівностороннього трикутника АСВ, рис. 1а, необхідно визначити координати цілі розташованої в точці О. Кожний БПЛА визначає кут між відрізком між двома сусідніми БПЛА та напрямком на ціль.

Необхідно визначення дальності $R_1 = [AO]$; $R_2 = [BO]$; $R_3 = [CO]$; Визначення дальності, наприклад D_1, D_2 здійснюється за допомогою теореми синусів. Причому, значення D_1, D_2, D_3 може бути здійснено декілька раз для визначення швидкості наземних цілей.

Визначення координат цілі $x_ц$, $y_ц$, $z_ц$ здійснюється шляхом рішення системи рівнянь ітераційним методом:

$$(x_ц - x_j)^2 + (y_ц - y_j)^2 + (z_ц - z_j)^2 = D_i{}^2,$$
$$j = \text{A, B, C}; \quad i = \overline{1,3}. \qquad (1)$$

Для підвищення точності визначення координат можна застосувати різницево-далекомірний метод рис 1b. Для цього застосовуються чотири

БПЛА, для кожного з яких вимірюється дальність до цілі, при цьому БПЛА розташований в т. D знаходиться в початку системи координат. Визначення координат цілі здійснюється шляхом рішення системи рівнянь:

$$(x_ц - x_j)^2 + (y_ц - y_j)^2 + (z_ц - z_j)^2 = D_i{}^2,$$
$$j = A, B, C; \ i = \overline{1,3}. \qquad (2)$$
$$x_D{}^2 + y_D{}^2 + z_D{}^2 = D_D{}^2.$$

Зазначимо що для цієї задачі далекомірний та різницево далекомірний методи є похідними з пеленгаційного методу, який далі розглянемо два варіанти застосування пеленгаційного методу.

Перший пеленгаційний метод, передбачає використання угрупування з чотирьох БПЛА рис. 1c). Кожен БПЛА розташований у вершинах квадрата, всі БПЛА розташовані на однієї висоті, та всі одночасно вимірюють пеленг на ціль, при чому якщо для попередніх методів для отримання максимальної точності визначення координат необхідно щоб проекція положення цілі обов'язково знаходилась в середині трикутника. то для пеленгаційного методу такої вимоги не має.

З метою зменшення кількості БПЛА з 4 до 2 пропонується застосування другого пеленгаційного метода. Реалізація цього метода передбачає наявність тільки двох БПЛА рис. 1 d. які розташовані в точках A, B. За допомогою системи взаємного вимірювання відстані [3] між БПЛА, відстань $|AB|$ відома. Ще однієї умовою застосування другого пеленгаційного метода є умова рівності висот польоту кожного з двох БПЛА.

Крім того, обов'язковою умовою досягнення високої точності визначення координат наземних цілей є те що, пеленг на ціль на борту БПЛА не повинен вимірюватись в градусах, або в радіанах, ці значення нелінійне зв'язані з прямокутною системою координат, а тільки в направляючих косинусах, це зменшує помилку вимірювання координат цілі.

Відстань між БПЛА визначається ланкою підрозділу розвідки, батальйонна або бригадна.

Література

1. Матричные радиометрические корреляционно-экстремальны системы навигации летательных аппаратов.–Х.: Изд-во ООО «Щедрая усадьба плюс», 2014– 372 с. ISBN 978-617-7188-XX-X.
2. О.В. Майстренко і інш. Визначення координат наземних цілей з використанням малогабаритних БПЛА на основі вдосконаленого псевдодальномірного методу Національна академія сухопутних військ імені гетьмана Петра Сагайдачного, Львів. DOI: https://doi.org/10.33577/2312-4458.22.2020.43-47.
3. Y. Yakornov O.Tsukanov Estimation of Motion Parameters of Unmanned Aerial Vehicles of Wireless Sensor Networks Based on the Least Squares Method with a Fractional Taylor Series in a "Sliding Window", International Scientific and Technical Conference - Modern Challenges in Telecommunications MCiT 2021: Progress in Advanced Information and Communication Technology and Systems pp 419–435.

УДК 621.396.946

МЕТОД ПІДВИЩЕННЯ ПРОПУСКНОЇ ЗДАТНОСТІ НЕОДНОРІДНОЇ МОБІЛЬНОЇ СЕНСОРНОЇ МЕРЕЖІ

Новіков В.І., Лисенко О.І., Алєксєєва І.В.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: novikov1967@ukr.net, lysenko.a.i.1952@gmail.com

A METHOD OF INCREASING THE BANDWIDTH OF A HETEROGENEOUS MOBILE SENSOR NETWORK

The article describes a method of increasing the bandwidth of a heterogeneous mobile sensor network using flying information robots.

Неоднорідні мобільні сенсорні мережі (НМСМ) із застосуванням літаючих інформаційних роботів (ЛІР) 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 в умовах відсутньої або зруйнованої наземної інфраструктури [1].

ЛІР - це безпілотний літальний апарат, який призначено для виконання інформаційно-телекомунікаційних операцій у НМСМ. На даний час відомі методи підвищення пропускної здатності стаціонарних сенсорних мереж з використанням однієї чи декількох телекомунікаційних повітряних платформ [2-3]. Ці методи ґрунтуються на тому, щоб забезпечити зв’язність роз’єднаних зон стаціонарних наземних вузлів, коли вся мережа являється єдиним кластером, або на тому, щоб збільшити зв’язність наземної мережі. Проте на сьогодні недостатньо розв’язаною є задача підвищення пропускної здатності НМСМ із застосуванням ЛІР в умовах кластерної зв'язності та використання одного ЛІР згідно з критерієм мінімізації часу обльоту всіх проміжних вузлів маршруту (точок збору інформації).

Розроблено новий метод підвищення пропускної здатності НМСМ із застосуванням ЛІР. Запропоновано нову методику оперативного розрахунку координат проміжних точок маршруту руху ЛІР, який збирає інформацію з мобільних вузлів НМСМ. Знання цих точок маршруту дозволяє побудувати ЛІТ-траєкторії, що мінімізує час для збору інформації з мобільних сенсорів (МС).

Процедура розрахунку в реальному часі координат проміжних точок маршруту передбачає послідовне використання алгоритмів задля розв’язання навігаційної задачі, задачі кластеризації та задачі знаходження траєкторії обльоту точок збору інформації від кластерів НМСМ, що були сформовані на момент початку збору інформації.

Для вирішення задачі кластеризації розроблено спеціальний алгоритм, який використовує процедури кількісного розрахунку показників структурної та інформаційної зв’язності НМСМ. Ці показники враховують наявність не

тільки структурного зв'язку, а й гарантованого обміну інформацією між даною парою відправник-адресат. Для кількісної оцінки ступеня структурної та інформаційної зв’язності НМСМ запропоновано два показники: k-зв’язність та пропускна здатність мережі.

Розроблено алгоритм керування топологією мережі ЛІР для покращення показників структурної та інформаційної зв’язаності НМСМ.

Застосування евристичних прийомів задля створення початкових умов (першого наближення) дозволяє суттєво зменшити складність пошуку квазіоптимального розв’язку задачі розміщення ЛІР та підвищити ймовірність досягнення глобального максимуму за кількісними показниками структурно-інформаційної зв’язності.

Моделювання функціонування НМСМ із ЛІР здійснювалося на базі комп’ютерного середовища Maple. Для створення було використано наступні початкові дані: кількість мобільних сенсорів N = 8, 12 або 16, які були випадково розставлені на поверхні в межах зони розгортання $r \leq 10^6\ m^2$. Допустимі значення параметрів МС та ЛІР: $d^0 = 100\text{м}, D^0 = 300\text{м}, R = 200\text{м}, s^0 = 0.9, l^0 = 5$. Кількість ЛІР на операцію була К = 5. Для спрощення обчислень було визначено що середнє навантаження кожного МС $\overline{g_i} = 5$. Довжина пакета становила L = 1000 біт.

Використовуючи запропоновані алгоритми було отримано:

1) графік залежності показника структурної та інформаційної зв’язності (пропускної здатності мережі) від координат розташування одного ЛІР (рис. 1);

2) графік залежності пропускної здатності мережі U^T від кількості *K* ЛІР у випадку різної кількості *N* мобільних сенсорів та різного розміру зони розміщення *r* (рис. 2).

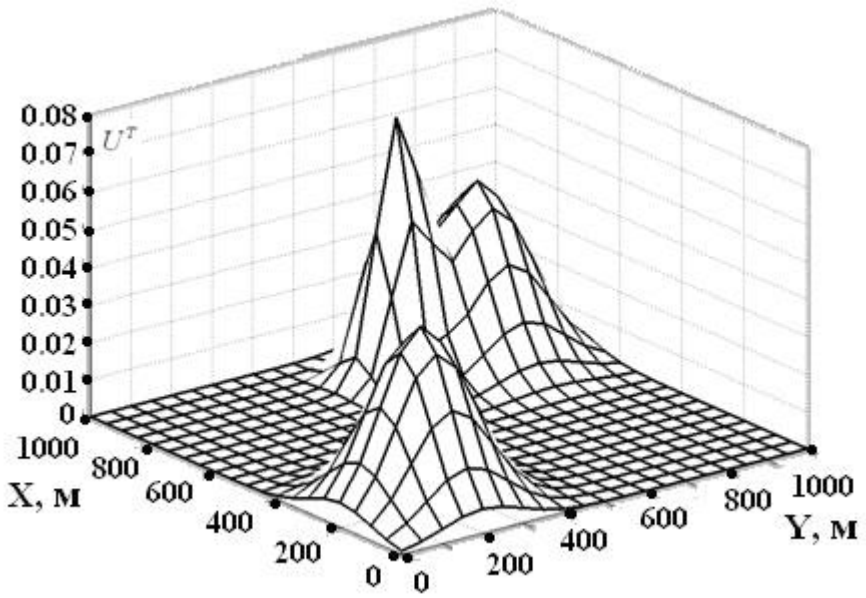
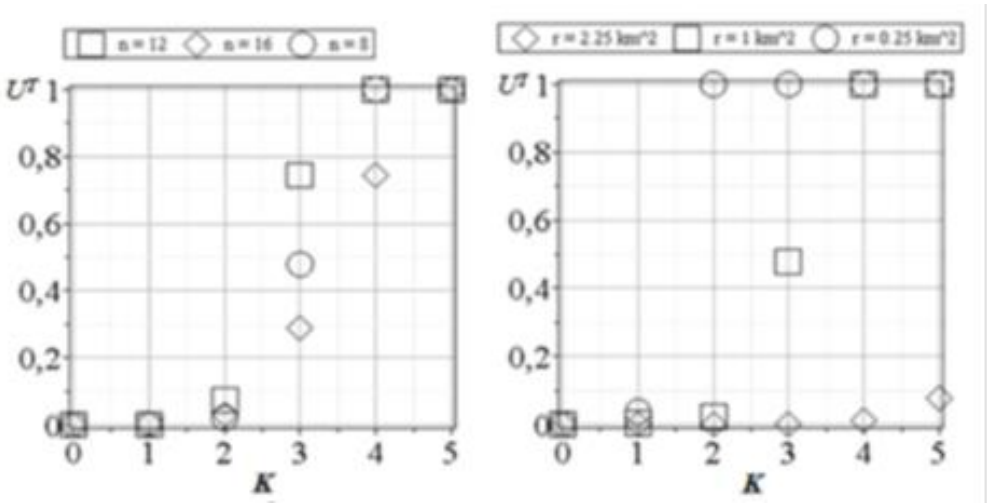


Рис.1. Залежність пропускної здатності мережі від координат знаходження одного ЛІР.

Аналіз Рис. 1 показує, що пропускна здатність має глобальний та декілька локальних максимумів. Тому, наприклад, коли ЛІР розташована у

точці глобального максимуму з координатами (302, 261), пропускна здатність досягає свого максимального значення. У цьому випадку використання одного ЛІР збільшує пропускну здатність мережі у 2-3 рази.



а) б)

Рис. 2. Залежність пропускної здатності мережі від кількості ЛІР.

Аналіз Рис. 2 показує, що пропускна здатність може бути збільшена шляхом використання кількох ЛІР. Ефективність використання комплекту ЛІР залежить від кількості МС у мережі та розміру зони розгортання. З більшою кількістю МС або з меншою ділянкою розгортання пропускна здатність буде більшою для обраної кількості ЛІР, оскільки сенсори матимуть сильнішу зв’язність між собою. ЛІР потрібно використовувати поки не буде досягнуто бажаного рівня зв’язності (пропускної здатності).

Практична цінність отриманих наукових результатів полягає в тому, що розроблений метод дозволяє кількісно оцінювати вплив мобільності вузлів НМСМ із ЛІР на тривалість зв’язності між МС; визначати раціональне положення ЛІР для досягнення якомога більших значень пропускної здатності НМСМ із ЛІР; здійснювати в режимі реального часу управління положенням ЛІР; підвищувати ефективність систем управління мережею ЛІР.

Література

1. Лисенко О.І. Методи оптимального керування рухом безпроводових сенсорних мереж із мобільними сенсорами та телекомунікаційними аероплатформами у зоні надзвичайної ситуації. Основи воєнно-теоретичних досліджень: нові реалії та технології: монографія в 4 т. Т.4: Дослідження операцій у військовій сфері. Розділ 6. / за заг. ред. професора І.С. Романченка. Київ: ЦНДІ ЗС України, 2022. – С. 162-204.
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.

УДК 004.738.5

ПОРІВНЯННЯ ХМАРНИХ СЕРВІСІВ З КЛАСИЧНИМИ КЛІЄНТ-СЕРВЕРНИМИ АРХІТЕКТУРАМИ

Руренко О.Г., Корельчук Д.Г.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: a.rurenko@gmail.com , denis.korelchuk@gmail.com

COMPARISON OF CLOUD SERVICES WITH CLASSIC CLIENT-SERVER ARCHITECTURES

The article analyzes cloud computing, accessibility, flexibility, privacy, security, and types of cloud computing models and their advantages over classic client-server architectures.

З розвитком технологій люди почали використовувати спільні обчислювальні ресурси, такі як сервери, сховища, мережі, додатки та інші хмарні сервіси, за допомогою хмарних обчислень, які також називають "хмарною" моделлю. Користувач може використовувати ці сервіси без додаткової допомоги провайдера. Історія хмарних обчислень протягається у далекі 60-ті роки минулого століття. Джон Маккарті, американський вчений, комп'ютерний фахівець та авторитет у галузі комп'ютерної теорії, вперше висловив ідею про те, що колись комп'ютерні обчислення будуть надаватися на кшталт комунальних послуг, у 1960 році, що дало початок поняттю "хмара" [1] .

Історія розвитку поділена на 4 етапи:

1. 1960-1990 – це етап виникнення ідеї дистанційного доступу до обчислювальних ресурсів. У цей період виникли перші системи віддаленого доступу до обчислювальних ресурсів, такі як термінальні сервери та системи дистанційного доступу. Однак, вони були дуже дорогими та вимагали значних витрат на обслуговування.

2. 1990-2000 – період розвитку інтернету та збільшення доступності обчислювальних сервісів. У цей період з’являються перші інтернет-сервіси, та велика кількість веб-сайтів. Компанії починають використовувати сервери на віддалених центрах обробки даних(дата центрах),що дозволяло отримувати доступ до більш потужних обчислювальних ресурсів.

3. 2000-2010 - розвиток віртуалізації та поява перших хмарних платформ. У цей період з'явилися перші віртуальні машини, що дозволяли розділити фізичний сервер на декілька віртуальних. Це дозволило зменшити витрати на обслуговування серверів та збільшити їх ефективність. Почали з'являтися перші хмарні платформи, такі як Amazon Web Services, Google Cloud Platform та Microsoft Azure.

4. З 2010 – до сьогодення – зростання популярності та розширення

функціональності хмарних обчислень. У цей час з'являються нові технології та хмарні послуги що дозволяють використовувати хмарні обчислення більш ефективно.

Хмарні обчислення доступні в будь-який час і з будь-якої точки світу, де є підключення до Інтернету. Провайдери хмарних сервісів, такі як Amazon Web Services (AWS), Microsoft Azure та Google Cloud Platform, пропонують широкий спектр послуг та інструментів для обчислень, зберігання даних, роботи в мережі та забезпечення безпеки в хмарі. Доступ до цих послуг можна отримати на вимогу, що дозволяє компаніям і приватним особам збільшувати або зменшувати масштаби за потреби без необхідності інвестувати у фізичну інфраструктуру.[2] Доступність і надійність послуг хмарних обчислень залежать від угоди про рівень обслуговування (SLA) з провайдером, яка зазвичай гарантує певний рівень безвідмовної роботи та продуктивності. Хмарні обчислення пропонують високий ступінь гнучкості для бізнесу та приватних осіб, дозволяючи їм масштабувати ресурси за потреби без необхідності інвестувати у фізичну інфраструктуру. Ось деякі з аспектів гнучкості хмарних обчислень:

Масштабованість: Хмарні обчислення дозволяють компаніям легко масштабувати свої обчислювальні ресурси, збільшуючи або зменшуючи їх за необхідності, залежно від попиту. Це означає, що компанії можуть швидко реагувати на зміни попиту та уникати надмірного виділення ресурсів.

Економічна ефективність: Хмарні обчислення є економічно вигідною альтернативою інвестиціям у фізичну інфраструктуру. Компанії можуть платити лише за необхідні їм ресурси та уникати витрат, пов'язаних з обслуговуванням та модернізацією обладнання.

Географічна гнучкість: Хмарні обчислення дозволяють компаніям отримувати доступ до своїх додатків і даних з будь-якої точки світу, якщо у них є підключення до Інтернету. Це означає, що компанії можуть легко розширювати свою діяльність у нових географічних регіонах без необхідності інвестувати у фізичну інфраструктуру.

Спритність: Хмарні обчислення дозволяють компаніям швидко розгортати нові програми та послуги, не турбуючись про базову інфраструктуру. Це дозволяє компаніям бути більш гнучкими та швидко реагувати на мінливі ринкові умови.

Мультихмарна гнучкість: Хмарні обчислення також пропонують можливість використовувати декілька хмарних провайдерів або хмарних сервісів. Це може забезпечити бізнесу більшу гнучкість з точки зору вартості, доступності та продуктивності.

Загалом, гнучкість хмарних обчислень є однією з їхніх ключових переваг, що дозволяє компаніям і приватним особам швидко адаптуватися до мінливих вимог і ринкових умов.

Хмарні обчислення призначені для забезпечення конфіденційності та безпеки даних за допомогою різних механізмів захисту. Використання заходів безпеки хмарних технологій, таких як шифрування, контроль доступу та протоколи мережевої безпеки, допомагає захиститися від несанкціонованого доступу, витоку даних та інших загроз безпеці.

Згідно з Rittinghouse, J. W., & Ransome, J. F. (2016), безпека хмарних обчислень є спільною відповідальністю між хмарним провайдером і користувачем хмарних обчислень. Хмарні провайдери відповідають за безпеку інфраструктури, в той час як користувачі хмарних обчислень відповідають за безпеку своїх додатків і даних у хмарі.[3]

Автори також припускають, що використання гібридної хмарної моделі може допомогти поліпшити конфіденційність і безпеку хмарних обчислень. Зберігаючи конфіденційні дані локально або в приватній хмарі, компанії можуть зберігати більший контроль над своїми даними та обмежити ризик їх витоку.

Загалом, конфіденційність і безпека хмарних обчислень залежать від поєднання заходів безпеки, політик і найкращих практик, а також від спільної відповідальності між постачальниками хмарних послуг і користувачами.

Хмарні сервіси мають кілька переваг над класичними клієнт-серверними архітектурами. По-перше, вони забезпечують більшу гнучкість, оскільки користувачі можуть отримувати доступ до додатків і ресурсів з будь-якого місця з доступом до Інтернету. По-друге, вони надійніші, оскільки дані зберігаються на серверах з резервним копіюванням, що до збереження інформації в разі втрати даних на локальних пристроях користувачів. По-третє, вони дозволяють використовувати потужні обчислювальні можливості віддалених серверів для роботи з додатками та обробки великих обсягів даних, що не займатиме значну кількість ресурсів на локальних пристроях користувачів.

Література

1. Craig A. Lee, Robert B. Bohn, Martial Michel.(February 2020) The NIST Cloud Federation Reference Architecture., pp. 13,22.
2. Erl, T., Mahmood, Z., & Puttini, R. (2013). Cloud computing: Concepts, technology & architecture. Prentice Hall., pp. 43-45, 51-54.
3. Rittinghouse, J. W., & Ransome, J. F. (2009). Cloud computing: implementation, management, and security. CRC Press., pp. 162-170.

УДК 621.382

ВДОСКОНАЛЕННЯ АЛГОРИТМІВ СИНХРОНІЗАЦІЇ В МОБІЛЬНИХ СЕНСОРНИХ МЕРЕЖАХ

Вавринюк Д.С.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: increase.dv28@gmail.com

IMPROVEMENT OF SYNCHRONIZATION ALGORITHMS IN MOBILE SENSOR NETWORKS

The article provides some background information about mobile sensor networks and the importance of synchronization algorithms in these networks. It also provides information on why synchronization is crucial in mobile sensor networks. It also shows methods for improving synchronization algorithms in mobile sensor networks.

Мобільні сенсорні мережі (MSN) привернули до себе значну увагу в останні роки завдяки їх численним застосуванням у різних сферах, включаючи моніторинг навколишнього середовища, охорону здоров'я та промислову автоматизацію [1]. MSN - це сукупність мобільних датчиків, які взаємодіють один з одним для виконання певного завдання. Однак точність та ефективність даних, зібраних цими сенсорами, значною мірою залежить від синхронізації їхніх годинників. Алгоритми синхронізації в MSN відповідають за узгодження годинників різних сенсорів, що є важливим для таких завдань, як злиття даних, відстеження цілей та локалізація. У цьому звіті ми пропонуємо методи вдосконалення алгоритмів синхронізації в МСМ та оцінюємо їхню продуктивність та ефективність [2].

Алгоритми синхронізації в мобільних сенсорних мережах можна розділити на дві категорії: засновані на часі та засновані на подіях. Алгоритми на основі часу синхронізують годинники датчиків періодично, тоді як алгоритми на основі подій синхронізують годинники, коли відбуваються певні події [3]. До алгоритмів на основі часу належать протокол синхронізації для сенсорних мереж (TPSN) та алгоритм еталонної широкомовної синхронізації (RBS). Алгоритми на основі подій включають протокол синхронізації часу заповнення (FTSP) і протокол синхронізації з дифузією часу (T-Diff) [5].

Однією з головних проблем синхронізації в MSN є перекіс тактових частот [4], який спричинений змінами тактової частоти через зміни температури, коливання напруги живлення та недосконалість виробництва. Щоб вирішити цю проблему, деякі алгоритми синхронізації використовують адаптивні алгоритми для підстроювання тактової частоти з часом.

Іншою проблемою в MSN є мобільність вузлів, яка може спричиняти затримки і втрати пакетів. Для вирішення проблеми мобільності вузлів було запропоновано кілька алгоритмів синхронізації, таких як протокол синхронізації для сенсорних мереж (TPSN) та алгоритм еталонної

широкомовної синхронізації (RBS). TPSN використовує деревоподібну топологію для синхронізації годинників і зменшує споживання енергії, тоді як RBS використовує еталонні трансляції для досягнення субмікросекундної точності синхронізації [4].

Останні досягнення в алгоритмах синхронізації зосереджені на підвищенні точності та зменшенні енергоспоживання. Одним з таких методів є протокол TimeSync [6], який використовує комбінацію алгоритмів синхронізації на основі часу та подій для досягнення високої точності та енергоефективності.

Одним із запропонованих методів покращення алгоритмів синхронізації в мобільних сенсорних мережах є використання гібридних алгоритмів, які поєднують методи синхронізації на основі часу та подій. Ці гібридні алгоритми можуть підвищити точність при мінімізації споживання енергії. Іншим запропонованим методом є використання розподілених алгоритмів, які дозволяють сенсорам синхронізуватися з сусідніми сенсорами, а не покладатися на централізований центр синхронізації [7].

Таблиця 1. Порівняння точності синхронізації та енергоспоживання різних алгоритмів синхронізації.

Algorithm	**Synchronization Accuracy**	**Energy Consumption**
TPSN	Medium	High
RBS	High	Low
FTSP	High	High
T-Diff	High	Medium
TimeSync	High	Low
Hybrid	High	Low

У таблиці 1 [5] порівнюються точність синхронізації та енергоспоживання різних алгоритмів синхронізації. З таблиці видно, що гібридні алгоритми перевершують традиційні алгоритми на основі часу та подій за точністю та енергоспоживанням.

Запропоновані гібридні алгоритми та розподілені алгоритми [7] були реалізовані та оцінені в симуляційному середовищі за допомогою симулятора TOSSIM. Результати моделювання показали, що запропоновані алгоритми покращують точність синхронізації та зменшують споживання енергії порівняно з традиційними алгоритмами, що базуються на часі та подіях.

Таблиця 2. Порівняння традиційних алгоритмів синхронізації.

Algorithm	**Advantages**	**Disadvantages**
Time-based	Simple and easy to implement	Susceptible to clock skew and energy consumption
Event-based	More energy-efficient	Requires accurate detection of events
Flooding Time Synchronization Protocol	Accurate and energy-efficient	Limited scalability
Timing-sync Protocol	Accurate and energy-efficient	Limited scalability

Результати також показали, що точність розподілених алгоритмів сильно залежить від кількості сусідів, з якими може спілкуватися датчик. Зі збільшенням кількості сусідів точність синхронізації покращувалася, а споживання енергії зменшувалося. Однак існувала межа кількості сусідів, з якими міг спілкуватися датчик, через обмеження дальності зв'язку [6].

Таблиця 3. Порівняння запропонованих алгоритмів синхронізації.

Algorithm	**Advantages**	**Disadvantages**
T-Diff	Distributed and energy-efficient	Highly dependent on the number of neighbors
Hybrid Algorithm	Accurate and energy-efficient	Complex implementation
TimeSync	High accuracy and energy-efficient	Limited testing in real-world scenarios

Алгоритми синхронізації мають вирішальне значення для мобільних сенсорних мереж, щоб гарантувати, що дані мають точну часову мітку і є надійними для аналізу та прийняття рішень. Традиційні алгоритми, що базуються на часі та подіях, мають обмеження, такі як перекіс годинника та споживання енергії. Запропоновані рішення, такі як гібридні алгоритми та розподілені алгоритми, продемонстрували багатообіцяючі можливості для покращення точності синхронізації та зменшення споживання енергії. Однак точність розподілених алгоритмів сильно залежить від кількості сусідів, з якими може зв'язуватися датчик, і існує межа для цього через обмеження дальності зв'язку. Подальші дослідження можуть бути спрямовані на подолання цих обмежень і розробку більш ефективних алгоритмів синхронізації для мобільних сенсорних мереж [7-8].

Література

1. Elsabrouty, M., & Youssef, M. (2016). Time synchronization in mobile sensor networks: a survey. Journal of Sensor and Actuator Networks, 5, 1-30.
2. Ganeriwal, S., Kumar, R., & Srivastava, M. B. (2003, May). Timing-sync protocol for sensor networks. In Proceedings of the 1st international conference on Embedded networked sensor systems (pp. 138-149).
3. Maróti, M., Kusy, B., Simon, G., & Lédeczi, Á. (2004, April). The flooding time synchronization protocol. In Proceedings of the 2nd international conference on Embedded networked sensor systems (pp. 39-49).
4. A. Detti, C. Pisa, S. Salsano, N. Blefari-Melazzi, “Wireless Mesh Software Defined Networks (wmSDN),” IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Oct 2013, pp. 89–95.
5. Lenzen, C., & Wattenhofer, R. (2009, April). T-diff: time diffusion for time synchronization in wireless sensor networks. In Proceedings of the 7th international conference on Embedded networked sensor systems (pp. 99-112).
6. Zhou, Y., Mao, Y., & Li, B. (2019). TimeSync: A high-accuracy and energy-efficient synchronization protocol for mobile sensor networks. IEEE Internet of Things Journal, 6, 576-588.
7. Hsu, C. C., & Chang, Y. J. (2019). An efficient distributed algorithm for time synchronization in mobile wireless sensor networks. Wireless Networks, 25, 2527-2538.
8. Truong, C., & Kim, K. H. (2020). A new synchronization algorithm for wireless sensor networks. IEEE Transactions on Industrial Electronics, 67, 269-277.

УДК 621.396.6

EXPLORATION OF EMISSION OF RADIO WAVES FOR MEANS OF COMMUNICATION AND CONTROL OF UNMANNED AERIAL VEHICLES

Filimonchuk V.M.

National Aviation University, Ukraine

“ Faculty of Air Navigation, Electronics and Telecommunications ”

E-mail: filimonchukvaleria@gmail.com

ДОСЛІДЖЕННЯ ПОШИРЕННЯ РАДІОХВИЛЬ ДЛЯ ЗАСОБІВ ЗВ'ЯЗКУ БЕЗПІЛОТНИХ АВІАЦІЙНИХ СИСТЕМ

В статті досліджено поширення радіохвиль в реальних умовах для тропосферної і земної хвиль в залежності від напряму, стану середовища, відстані та потужності випромінювача для вирішення задач перехоплення бпла. Знайдено найбільш раціональні способи розрахунку поширення радіохвиль.

There are many different methods of prognostication of the emission of radio waves, but most of them are easy, but not accurate or accurate, but too difficult. In addition, the complexity is that conditions of emission of tropospheric and terrestrial waves differ.

So, the purpose of work was to explore emission of radio waves in real conditions for tropospheric and terrestrial waves depending on direction, environment, distance and emitter power to block UAV and find the most rational ways to calculate emission of radio waves.

To achieve the goals. I have to:

1. search for known methods of emission of radio waves.
2. choose that method that will be easy and accurate enough.

3. make physical modelling of the emission of radio waves in real conditions of using UAV.

The object of study was the phenomenon of the emission of radio waves in real conditions.

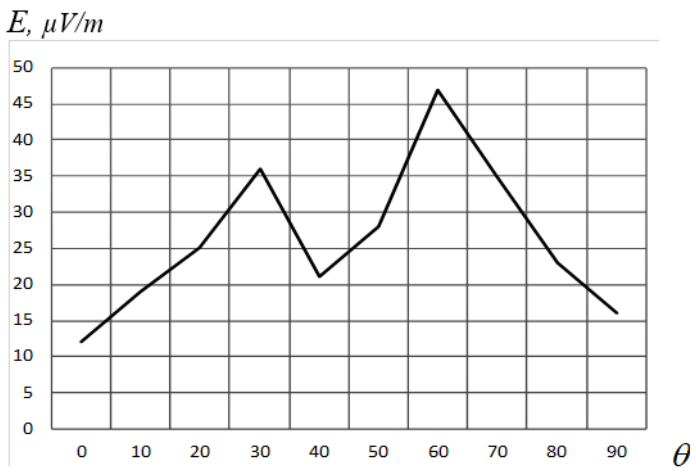
The subject of study was the method of determining the electric field strength of the radio wave, which can be used for rapid changes in UAV usage conditions.

In the course of my work, at first, I researched known methods of radio waves emission. For example, Okomura-Hata's method, COST-Hata's, Schulekyn Van-der-Pol's, Wallfish-Ikegami's, the model of perfect radio emission. I chose the last one, supplemented it with a multiplier of radio waves scattering in a standard troposphere and did theoretical calculations.

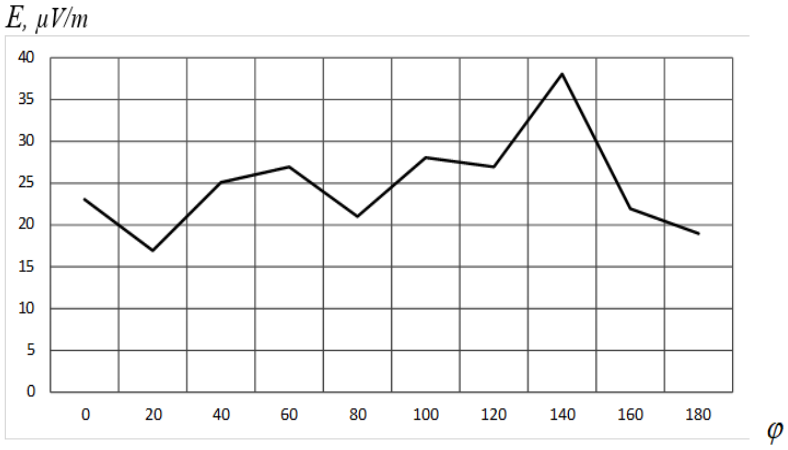
Using chosen methods, I calculated the distance of possible range of radio interception.

After this, to prove my results, I did an experiment using laboratory stand of electrodynamic model of surrounding, which is in the picture.

In the experiment I explored dependence of the intensity of the radio wave field on the direction in horizontal and vertical plane, which is shown on the graphics:



Pic 1. The electric field strength of the radiowave in vertical plane



Pic 2. The electric field strength of the radiowave in gorisontal plane

According to the results of my experiment, I found interference maxima and minima, that are the consequence of the influence of relief and subsoil. The values in the range of the maximum of radio wave field intensity show a possibility of strengthening or weakening the signal level, which impact on the distance of interception range of UAV. According to the average value, results are equal to those ones, that were done with taking electrodynamic scaling into account.

Conclusion:

1. not difficult, but accurate enough method of emission of tropospheric and terrestrial radio waves in real conditions of using UAV were analysed.

2. the experimental exploration using physical modelling of radio waves emission in real conditions of using UAV, that coincides with approximate calculation the distance of possible radio interception was done.

References

1. Безпілотні авіаційні комплекси: моногр. / В.Г. Башинський, В.Б. Бзот, Е.И. Жилин и др. – Запоріжжя, 2016. – 211 с.
2. Іванов В.О., Габрусенко Є.І., Сібрук Л.В. Теорія електромагнітного поля. Навчальний посібник. – К.: НАУ, 2017. – 336 с.
3. O.Lavrynenko, A.Taranenko, I.Machalin, Ye.I.Gabrousenko, I.Terentyeva, D.Bakhtiarov. Protected voice control system of UAV/ 2019 IEEE 5th International Conference Actual Problems of Unmanned Aerial Vehicles Developpement / Proceedings Kiev, October 22-24, 2019, pp. 295-298.

УДК 621.396

ОЦІНКА ПАРАМЕТРІВ РУХУ ГРУПИ ПОСТІЙНО МАНЕВРУЮЧИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Цуканов О.Ф., Якорнов Є.А.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: cukanov-o@ukr.net

ESTIMATION OF MOTION PARAMETERS OF A GROUP OF CONSTANTLY MANEUVERING UNMANNED AERIAL VEHICLES

A model for estimating movement parameters for maneuvering unmanned aerial vehicles based on a Kalman filter with limited memory is presented. The stability of operation is ensured by the correct selection of only one parameter, the value of which is determined by the results of simulation. Such a model can be easily adapted for any unmanned aircraft both for the task of estimating movement parameters and for solving escort tasks.

Інтенсивне використання на полі бою групи безпілотних літальних апаратів (БПЛА), наприклад, на базі квадрокоптерів передбачає, що кожен апарат функціонує в режимах постійного маневру. Тому одним із завдань, яке необхідно вирішувати на наземному пункті управління, - визначення параметрів руху (ПД) таких БПЛА з високою точністю.

Відомо [1] рішення для рівномірного руху БПЛА на основі опису ПД системою диференціальних рівнянь. Розглянемо застосовність даної методології з метою оцінки ПД апаратів із постійним маневром.

Сформулюємо завдання оцінки ПД маневрують БПЛА при їхньому квазіоднорідному розподілі в просторі наступним чином.

На підставі наявної інформації про координати $\widetilde{x_i}$, $\widetilde{y_i}$, $\widetilde{z_i}$ та їх середньоквадратичні помилки $\widetilde{\sigma x_i}$, $\widetilde{\sigma y_i}$, $\widetilde{\sigma z_i}$ необхідно визначити ПД: оцінку вектора стану (ВС) $\overrightarrow{X_n}$, координати $\widehat{x_i}$, $\widehat{y_i}$, $\widehat{z_i}$, похідні (швидкості) $\widehat{\dot{x}_i}$, $\widehat{\dot{y}_i}$, $\widehat{\dot{z}_i}$ і кореляційні матриці помилок (КМО) K_n, і надалі після чергового етапу вимірювань відстаней між сусідніми БПЛА проводити їх уточнення.

Для отримання високоточних оцінок ПД у разі маневру БПЛА при багаторазових вимірах скористаємося моделлю оцінювання з урахуванням фільтра Калмана [2]. При цьому припускаємо, що помилки визначення координат які, у свою чергу, є вхідною інформацією для уточнення розташування елементів групи мають закон розподілу помилок, який у загальному випадку відрізняється від нормального.

Початковими умовами моделі оцінювання є ВС X_{n-1} та апріорна КМО K_{n-1} на n-1 кроці вимірювань.

ВС можна записати у вигляді:

$$X_{in}{}^{T} = |x_{in},\ \dot{x}_{in},\ y_{in},\ \dot{y}_{in}, z_{in}, \dot{z}_{in}|,$$
$$Y_{in}{}^{T} = |\widetilde{x_{in}}\ ,\ \widetilde{y_{in}},\ \widetilde{z_{in}}|. \quad (1)$$

Тоді екстрапольоване значення ВС у загальному вигляді можна записати

$$X_{\text{in}}^{\text{e}} = F_{in,n-1}X_{in-1} + G_{n-1}U_{n-1}, \quad (2)$$

де $F_{in,n-1}$ - матриця екстраполяції, G_{n-1} – матрица управління,
$U_{\text{n}-1}{}^{T} = |0 \quad 0 \quad 0 \quad a_{x,n-1} \quad a_{y,n-1} \quad a_{z,n-1}|$ – вектор управління, в якому $a_{x,n-1} \quad a_{y,n-1} \quad a_{z,n-1}$ – прискорення БПЛА за координатами.

За аналогією з (2) екстрапольовану апріорну оцінку КМО можна також подати наступним чином

$$K_{in}^{e} = F_{in,n-1}\, K_{in-1} F_{in,n-1}{}^{\text{T}} + \gamma \text{G}_{\text{n}-1}\, S_{n-1} G_{\text{n}-1}^{T}, \quad (3)$$

де K_{in-1} – екстрапольована апріорна КМО, γ – параметр стійкості.
де K_{in-1} – екстрапольована апріорна КМО, γ – параметр стійкості.

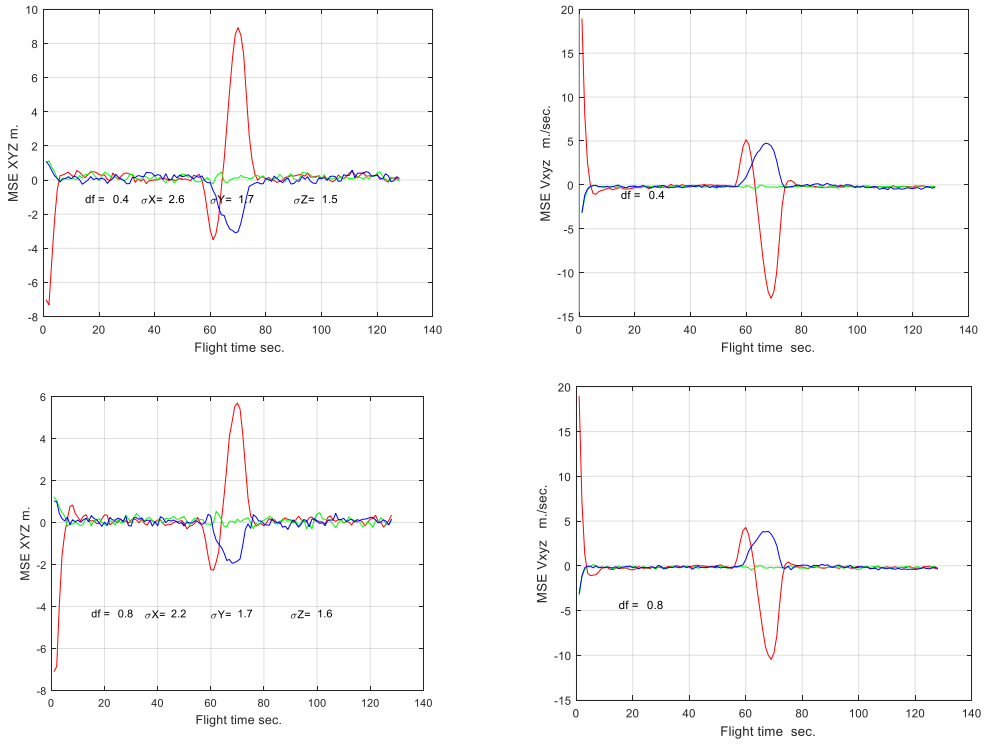
Оцінка ВС стану та КМО оцінювання показана в [3]. Співвідношення (2)-(3) дозволяють забезпечити стійке оцінювання ВС при раптовій зміні траєкторії руху БПЛА. Оцінки ВС БПЛА включають координати $|\widehat{x_{in}},\ \widehat{y_{in}},\ \widehat{z_{in}},\ |^{\text{T}}$. При цьому помилки визначення координат σx_i , σy_i , σz_i без урахування кореляційних моментів можуть бути графічно представлені у вигляді еліпсоїда, в центрі якого знаходиться БПЛА.

Аналогічно - за швидкісними складовими ВС $|\widehat{\dot{x}_{in}},\ \widehat{\dot{y}_{in}},\ \widehat{\dot{z}_{in}}|$ помилки визначення швидкостей за координатами $\sigma\dot{x}_i, \sigma\dot{y}_i, \sigma\dot{z}_i$ також можна подати у вигляді еліпсоїда, але з великими розмірами за абсолютними величинами.

Якщо "обсяг" таких паралелепіпедів буде досить малим, можна говорити про стійкий автосупровід кожного БПЛА з високою точністю. Якщо такого високоточного автосупроводу не потрібно, оцінюються лише координати розташування.

Стійкість оцінювання ВС БПЛА забезпечується "примусовим збільшенням" значень діагональних елементів $\sigma\dot{a}_x{}^2, \sigma\dot{a}_y{}^2, \sigma\dot{a}_z{}^2$ матриці $G_{in,n-1}$ шляхом множення на параметр γ. Таким чином, константами в моделі (3) є параметр γ і величина Δt - час між вимірюваннями відстані між БПЛА. У зв'язку з цим, при моделюванні можна заздалегідь поставити елементи КМО вектору управління S_{n-1} (2) для забезпечення стійкості та необхідної точності оцінювання. Для перевірки запропонованої моделі оцінки ПД БПЛА, що постійно маневрує, використовувалася модель руху на основі реальних технічних характеристик апарату типу "Орлан".

Деякі результати моделювання траєкторій польоту БПЛА при його розвороті на 90^0 для різних значень параметра представлені на малюнку (при γ=0, має місце розбіжність процесу оцінювання, тобто, фільтр Калмана не стійкий).



$\gamma = 0.4$

$\gamma = 0.8$

Для значень $0.4 \leq \gamma \leq 0.8$ запропонована модель забезпечує стійкість процесу оцінювання. Аналіз величини помилки оцінювання за координатами і швидкостями із усередненням по 100 реалізаціям показує, що у ділянці маневру максимальна помилка за координатами становить 18 м при γ=0.1, а мінімальна - 5 м. при γ=0.4.

Максимальна помилка за швидкостями становить 18 м/с. при γ=0.1, а мінімальна - 10 м/с. при γ=0.4. Оптимальне значення з допомогою якого отримані такі помилки оцінювання дорівнює 0.8.

При цьому значення забезпечується стійке оцінювання ПД БПЛА при досягненні мінімального значення помилки визначення ВС в середньому за 8 кроків оцінювання.

Література

1. Товкач И. О., Жук С. Я. Адаптивная фильтрация параметров движения БПЛА по данным сенсорной сети на основе измерения мощности принимаемого сигнала. Вестник НТУУ «КПИ». Серия Радиотехника. Радиоаппаратостроение. 2017. № 69. с. 41-48.
2. Grewal M.S., Andrews A.P., «Kalman Filtering — Theory and Practice Using MATLAB», Wiley, 2001.
3. Y. Yakornov, O. Tsukanov Estimation of the Motion Parameters of Unmanned Aircraft of Wireless Sensor Networks Using Taylor Fractional Series. 2021

IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (IEEE UkrMiCo'2021), Kyiv, Ukraine, November 29 – December 3, 2021, pp. 212-215.

УДК 621.396.96:004.738.5:004.738.7

МЕТОДИ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ MIMO В МОБІЛЬНИХ СЕНСОРНИХ МЕРЕЖАХ

Тимофеєв Є.М., Лисенко О.І.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: timofeeevzh@gmail.com, lysenko_home@ukr.net

METHODS OF APPLYING MIMO TECHNOLOGY IN MOBILE SENSOR NETWORKS

The technology of Multiple-Input/Multiple-Output (MIMO) is a promising direction in wireless communications, which allows for increased throughput and more robust signal reception in noisy and distorted environments. This paper examines the methods and approaches for the application of MIMO technology in mobile sensor networks. The paper analyzes the potential effectiveness and challenges of using MIMO in mobile sensor networks, and provides examples of MIMO application in sensor networks.

Технологія множинного введення/виведення (MIMO) є перспективним напрямком в бездротових комунікаціях, який дозволяє підвищити пропускну здатність та забезпечити більш стійкий прийом сигналів в умовах шуму та спотворень. У цій роботі розглядаються методи та підходи до застосування технології MIMO в мобільних сенсорних мережах. В роботі аналізується потенційна ефективність при застосуванні MIMO в мобільних сенсорних мережах, а також наводяться приклади застосування MIMO у сенсорних мережах.

В останні роки мобільні сенсорні мережі стали дедалі більш поширеними в різних сферах життя, таких як медицина, спорт, промисловість та інше. Ці мережі використовують датчики, щоб збирати різноманітні дані, наприклад, температуру, вологість, рівень шуму та інші параметри. Проте, при розвитку мобільних сенсорних мереж виникають різні проблеми, такі як недостатня пропускна здатність, обмежена енергоефективність, складність маршрутизації та інші.

Одним з методів, що допомагають вирішувати ці проблеми, є використання технології MIMO (Multiple Input Multiple Output). Технологія MIMO використовується в багатьох радіозв'язкових системах, включаючи Wi-Fi та мобільний зв'язок. Вона дозволяє використовувати більше однієї антени для передачі та отримання сигналів, що дозволяє збільшити кількість передавальних каналів та покращити якість сигналу. У мобільних сенсорних мережах, використання технології MIMO дозволяє підвищити пропускну здатність, зменшити споживання енергії та покращити маршрутизацію даних.

Отже, роль технології MIMO у мобільних сенсорних мережах полягає в тому, що вона допомагає вирішувати проблеми, пов'язані з обмеженою пропускною здатністю, енергоефективністю та маршрутизацією даних [1], [2].

Таблиця 1. Переваги та недоліки використання MIMO в мобільних сенсорних мережах.

Переваги	Недоліки
Покращена пропускна здатність	Високі вимоги до апаратного забезпечення
Зниження енергоспоживання	Складність реалізації
Покращення якості передачі даних	Обмеження покриття

Методи застосування технології MIMO (Multiple Input Multiple Output) в мобільних сенсорних мережах можуть бути різними, але в основному мають на меті покращити продуктивність та якість передачі даних, зменшити інтерференцію та забезпечити більш високу надійність передачі даних. Найпоширеніші методи застосування MIMO в мобільних сенсорних мережах [3]:

- Просторове кодування (Space-Time Coding);
- Просторове мультиплексування (Spatial Multiplexing);
- Масивне MIMO (Massive MIMO);
- Частотне MIMO (Frequency MIMO).

Просторове кодування є методом, який забезпечує резервні копії даних, що передаються, та покращує якість передачі даних у мережі. Перевагами цього методу є зменшення впливу втрати даних на передачу та забезпечення більш високої надійності передачі даних. Однак, недоліком є погіршення пропускної здатності мережі.

Просторове мультиплексування дозволяє використовувати кілька антен для передачі даних з різних потоків. Використання кількох антен дозволяє збільшити пропускну здатність мережі та зменшити інтерференцію. Перевагами цього методу є збільшення пропускної здатності мережі та зменшення інтерференції. Недоліком є менша надійність передачі даних.

Масивне MIMO використовує велику кількість антен для передачі та отримання даних, що дозволяє зменшити вплив шумів та інтерференції на передачу даних та забезпечує більш високу надійність передачі даних. Перевагами цього методу є забезпечення високої пропускної здатності та низької затримки передачі даних. Однак, недоліком є складність реалізації та високі вимоги до обчислювальних ресурсів [4].

Частотне MIMO використовується для забезпечення високої пропускної здатності та низької затримки передачі даних шляхом використання кількох частотних діапазонів. Перевагами цього методу є забезпечення високої пропускної здатності та низької затримки передачі даних, а також підвищення надійності передачі даних. Недоліком є збільшення вимог до обчислювальних ресурсів та складність реалізації.

Один з найбільш популярних прикладів використання MIMO в мобільних сенсорних мережах – це використання технології MIMO в стандарті LTE. У LTE використовується технологія просторового мультиплексування (Spatial Multiplexing), що дозволяє передавати дані на кількох потоках з використанням кількох антен базової станції та кінцевого пристрою. Це забезпечує високу пропускну здатність та ефективність передачі даних в мобільних мережах [5].

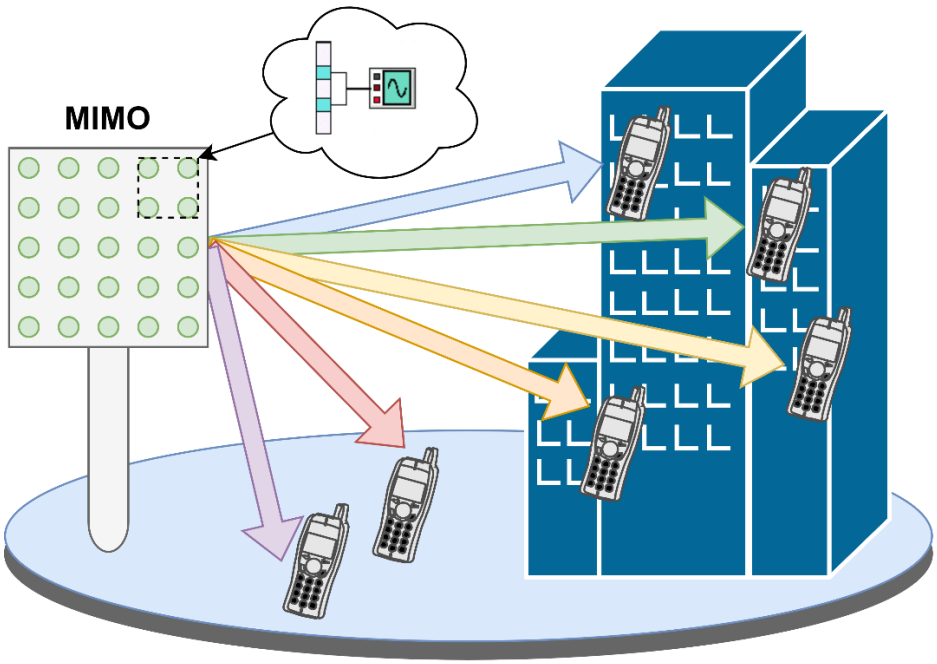


Рис. 1. Сценарій використання MIMO в 5G.

У сучасних мобільних мережах також використовуються MIMO для забезпечення високошвидкісної передачі даних на високих частотах. Наприклад, технологія Massive MIMO використовується в мережах 5G для забезпечення високої пропускної здатності та зниження затримки передачі даних. У мережах 5G Massive MIMO дозволяє використовувати більше антен на базовій станції та більшу кількість користувачів одночасно, забезпечуючи кращу якість обслуговування та швидкість передачі даних [4].

Ще одним прикладом використання MIMO є мережі Wi-Fi. Технологія просторового кодування (Space-Time Coding) використовується для забезпечення надійної передачі даних в мережах Wi-Fi. Зокрема, технологія MIMO використовується в стандарті Wi-Fi 802.11n, що забезпечує більш високу пропускну здатність та стабільність зв'язку у порівнянні зі стандартом 802.11b/g.

Також MIMO використовується в сенсорних мережах для забезпечення ефективної передачі даних з сенсорів до центрального вузла мережі. Наприклад, у мережах бездротового зчитування показників енергоспоживання (Wireless Smart Metering), MIMO дозволяє передавати дані з кількох сенсорів одночасно з використанням кількох антен базової станції, що забезпечує високу надійність передачі даних та ефективність мережі [5].

Все більш критичним параметром у мобільних мережах стає швидкість передачі даних. MIMO здатна забезпечувати передачу даних на великій відстані та з високою швидкістю, що дозволяє мобільним пристроям працювати з більшим обсягом даних та робити це швидко і ефективно. Крім того, MIMO може бути використана для поліпшення якості зв'язку, зменшення шумів та інтерференцій в мобільних мережах.

Технологія MIMO є ключовим елементом у сучасних мобільних мережах, а особливо в мережах 5G. Вона дозволяє мобільним пристроям працювати з більшою кількістю антен та забезпечує ефективну передачу даних, що необхідно для нових високошвидкісних додатків, таких як відеоконференції та стрімінгові сервіси.

Отже, можна зробити висновок, що MIMO є дуже ефективною технологією для покращення ефективності мобільних мереж. Вона забезпечує швидку передачу даних на великій відстані та підвищує якість зв'язку. У майбутньому, MIMO буде ще більш важливою для мобільних мереж, особливо в контексті розвитку нових високошвидкісних додатків та послуг.

Література

1. Li, J., Zhang, Y., Chen, X., Li, K., & Li, X. (2017). Multiuser MIMO transmission in wireless sensor networks: A survey. IEEE Communications Surveys & Tutorials, 19(4), 2655-2680.
2. Khan, M. A., Jeon, M., & Kim, K. (2019). A review of MIMO-based wireless sensor networks. Journal of Network and Computer Applications, 126, 33-47.
3. Abbasi, Q. H., Zhang, H., & Merabti, M. (2016). MIMO techniques for wireless sensor networks: a survey. Wireless Networks, 22(6), 1867-1888.
4. Lu, L., Li, G. Y., Swindlehurst, A. L., Ashikhmin, A., & Zhang, R. (2014). An overview of massive MIMO: Benefits and challenges. IEEE Journal of Selected Topics in Signal Processing, 8(5), 742-758.
5. Nguyen, T. H., Nguyen, C. T., Nguyen, H. H., & Kim, Y. (2018). A survey of multiple antenna techniques in wireless sensor networks. Sensors, 18(9), 2847.

УДК 004.725.5:621.396:631.234

ПОРІВНЯННЯ ТЕХНОЛОГІЙ LI-FI ТА WI-FI У ВИКОРИСТАННІ ДЛЯ ТЕПЛИЧНОГО ГОСПОДАРСТВА

Руденко А.А., Курдеча В.В.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: anastasiarudenko078@gmail.com

COMPARISON OF LI-FI AND WI-FI TECHNOLOGY IN GREENHOUSE FARMING

The purpose of the publication is to compare Wi-Fi and Li-Fi technologies in the structure of a "smart" greenhouse based on Internet of Things technology. In particular, the disadvantages and advantages of these technologies are determined.

У наш час, новітні технології допомагають збирати великі масиви даних для більш кращого керування ростом рослин. Для передачі цих масивів даних та подальшої обробки потрібно побудувати інфокомунікаційну мережу, що буде відповідати всім пунктам, були зазначені вище.

З безпроводових мереж зараз панує технологія Wi-Fi, але існує і інша технологія – Li-Fi (від англ. Light Fidelity). Wi-Fi використовує для передачі радіохвилі діапазону 2,4 ГГц, 5ГГц та 6ГГц. Натомість, Li-Fi використовує для передачі даних видимий спектр світла.

Метою публікації є порівняння технологій Wi-Fi та Li-Fi в структурі «розумної» теплиці на основі технології Інтернету речей. Зокрема визначено недоліки та переваги цих технологій в зазначеній галузі.

1) Wi-Fi.

Якщо порівнювати Wi-Fi з технологіями 3G, 4G або LTE, це — дешева технологія, що забезпечує гарну пропускну здатність та низьке енергоспоживання.

Переваги:

• Дуже поширена, майже всі пристрої мають адаптери для цієї технології.

• Нескладна в настроюванні для пересічного користувача.

• Легко проникає через перешкоди.

Недоліки:

• Низька швидкість, порівняно з Li-Fi та провідною Ethernet.

• В місцях великого скупчення людей, де є дуже багато мереж Wi-Fi, що працюють на одній частоті, займаються всі канали передачі і швидкість сильно падає.

• Wi-Fi, що працює на частоті 2,4-2,7 ГГц “конфліктує” з технологіями, такі як, Bluetooth тому, швидкість передачі при використанні обох технологій падає.

2) Li-Fi.

Ця технологія теоретично дешевша, ніж Wi-Fi, але має ряд особливостей, що роблять її не такою розповсюдженою, ніж Wi-Fi. Перспективні напрямки використання Li-Fi: оранжереї, теплиці та кафе з великою кількістю рослин.

Переваги:

• Висока швидкість – 1 Гбіт/сек, в той час коли як швидкість Wi-Fi 150 Мбіт/сек, Bluetooth – 3 Мбіт/сек. [1]

• Достатньо проста по своїй суті та дешева технологія.

• Світло має набагато більшу ширину спектра, ніж у Wi-Fi.

•Поєднання світла та мережі в світлодіод робить цю технологію ще економнішою.

• Так як передача енергії здійснюється в межах кімнати, перехопити дані, знаходячись поза кімнатою буде неможливо.

Недоліки:

• Передача інформації можлива тільки в зоні прямої видимості. Через непрозорі предмети– швидкість передачі сильно падає.

• Непоширена технологія, купити пристрій, що підтримуватиме Li-Fi дуже важко.

•Отримати інформацію можна за допомогою видимого світла, то відправити її потрібно за іншою технологією.

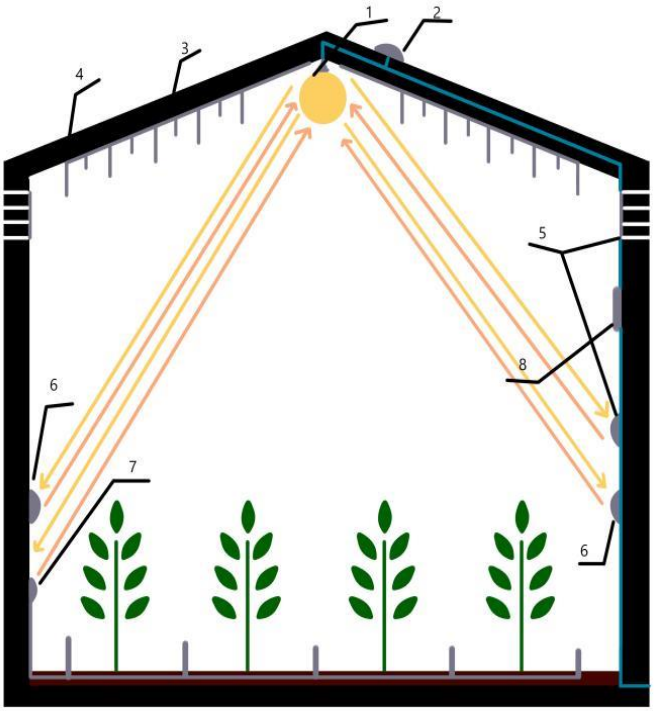


Рис. 1. Макет побудови теплиці
1– передатчик Li-Fi; 2 – датчик зовнішнього середовища; 3 – система оприскування; 4 – система поливу; 5 – датчик повітря та система вентиляції; 6 – датчики освітленості; 7 – датчик стану грунту; 8 – контролер.

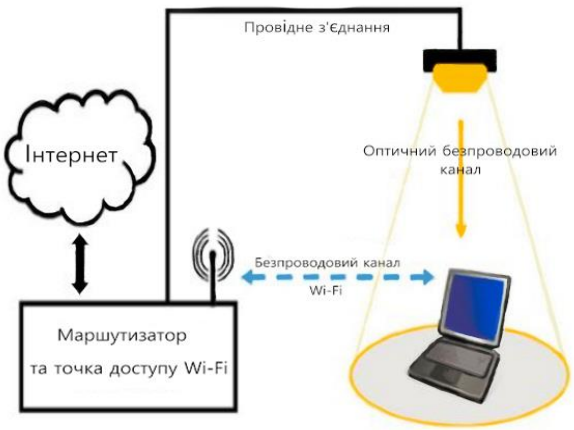


Рис. 2. Організація мережі Li-Fi(+Wi-fi)[3].

Зараз, сільське господарство є однією з галузей економіки, що наносить найсильніший вплив на екологію. Учені з Інституту землеустрою УААН провели оцінку екологічної стабільності землекористування. І з нього виявилось, що тільки Закарпатська область є стабільною [2]. Для поліпшення ситуації, можна використовувати технології Інтернету речей та технології Li-Fi. Потрібно зазначити, що технології Li-Fi будуть ефективними тільки в тепличному господарстві, бо велика кількість сонячного світла буде створювати перешкоди для передачі інформації.

Автоматизована теплиця – теплиця, що може сама контролювати свій мікроклімат, який складається з контролю температури, контроль вологості грунту, контролю освітлення, контролю повітря, контроль комах. Можна запропонувати такий варіант організації мережі: використати властивість світла огинати перешкоди, але швидкість передачі впаде, при цьому інформація з датчиків не потребує високої швидкості передачі даних.

Отримання даних на контролер буде за допомогою Li + Wi-Fi — технологія, в якій поєднується Li-Fi і Wi-Fi. [3]

Можна сказати, що Li-Fi – багатообіцяюча технологія, якій можна буде знайти багато застосувань. Управління за допомогою Інтернету речей та Li-Fi(+Wi-fi) може вирішити проблему недоцільного використання мінеральних добрив, які шкодять не тільки екології а і здоров'ю людини [2].

Література

1. Lamya I. Albraheem Lamia H. Alhudaithy, Afnan A. Aljaser, Muneerah R. Aldhafian, Ghada M. Bahliwah. TOWARD DESIGNING A LI-FI-BASED HIERARCHICAL IOT ARCHITECTURE [Електронний ресурс]/Publisher:IEEE/. – 2018. – 14 с. – Режим доступу : URL : https://ieeexplore.ieee.org/document/8413064.
2. Бурляй А. П., Бурляй О. Л., Непочатенко О. А.ВПЛИВ ДІЯЛЬНОСТІ СІЛЬСЬКОГОСПОДАРСЬКИХ ПІДПРИЄМСТВ НА НАВКОЛИШНЄ ПРИРОДНЕ СЕРЕДОВИЩЕ[Електронний ресурс]/Науковий вісник Ужгородського національного університету/. –2018.–5с.–Режим доступу: URL :
http://www.visnyk-econom.uzhnu.uz.ua/archive/20_1_2018ua/16.pdf
3. Saily P. Bhanse, Savita R. Pawar LI+WI-FI:THE FUTURE OF INTERNET OF THINGS [Електронний ресурс]/2018 3rd International Conference on Communication and Electronics Systems (ICCES)/.–2018.–6с.–Режим доступу: URL :

   https://ieeexplore.ieee.org/document/8724051
4. J. Yamnenko, L. Globa, V. Kurdecha and A. Zakharchuk, "Data Processing in IoT Systems based on Fuzzy Logics," 2019 Modern Electric Power Systems (MEPS), Wroclaw, Poland, 2019, pp. 1-4, doi: 10.1109/MEPS46793.2019.9395055.

УДК 621.396.96

ПІДСИСТЕМА ДЕКОРЕЛЯЦІЇ СИГНАЛІВ ВІД ПАСИВНИХ ЗАВАД В СУЧАСНИХ РАДІОЛОКАЦІЙНИХ СИСТЕМАХ

Терещенко О.В., Чмельов В. О.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: alexandr.t.v.188@gmail.com

SUBSYSTEM OF DECORRELATION OF SIGNALS FROM PASSIVE INTERFERENCES IN MODERN RADARS

A complex approach to the construction of a surveillance radar subsystem is proposed to simultaneously solve the problems of compensating for the effects of passive interference and improving the signal-to-noise ratio to increase the effectiveness of the radar.

Застосування БПЛА стало одним із основних джерел небезпеки об’єктам критично-важливої інфраструктури. Широкий спектр моделей сучасних БПЛА, призвів до появи нового класу складних радіолокаційних об’єктів, виявлення яких ускладнене через їх малі розміри, малу швидкість руху, та застосування для їх виготовлення радіопрозорих матеріалів [1].

Крім того, тактика застосування БПЛА характеризується використанням їх на малих висотах, на фоні місцевих предметів, різкою зміною напрямку і швидкістю руху, зависанням на одному місці в повітрі, що суттєво ускладнює роботу радіолокаційних систем (РЛС) щодо їх виявлення.

Тому постає завдання розробки нових вузлів радіолокаційних систем, які повинні комплексно і одночасно вирішувати декілька завдань в процесі виявлення радіолокаційних об’єктів в складних умовах.

Одна з проблем в роботі РЛС, це захист від пасивних завад різної фізичної природи. Джерелами завад можуть бути: підстилаюча поверхня землі, штучні дипольні відбивачі, метеорологічні утворення – туман, сніг, хмари, тощо [2].

Вирішення задачі захисту РЛС від пасивної завади зводиться до декореляції (вибілення) сигналу, відбитого від пасивної перешкоди, тобто приведення його характеристик до характеристик білого шуму.

Класичним відомим підходом є застосування черезперіодного компенсатора, що реалізується цифровим трансверсальним фільтром з скінченною імпульсною характеристикою [3], структурна схема зображена на рис. 1.

На схемі фільтру, h_i - вагові коефіцієнти, z^{-1} - затримка сигналів на інтервал T, де T - період випромінювання зондуючого сигналу РЛС.

Амплітудно-частотну характеристику цього фільтра $|K_0(f)|$ виберемо так [1], щоб спектральна щільність потужності пасивних завад на його виході $N(f)|K_0(f)|^2$ не залежала від частоти, або $N(f)|K_0(f)|^2 = const = C$

$$K_0(f) = \sqrt{\frac{C}{N(f)}} \tag{1}$$

Таким чином, бачимо, що на виході фільтру буде збільшена потужність білого шуму. В таких умовах, відношення сигнал шум буде погіршене, і ймовірність виявлення відбитого сигналу від радіолокаційного об’єкту, типу БПЛА, на фоні буде суттєво знижена.

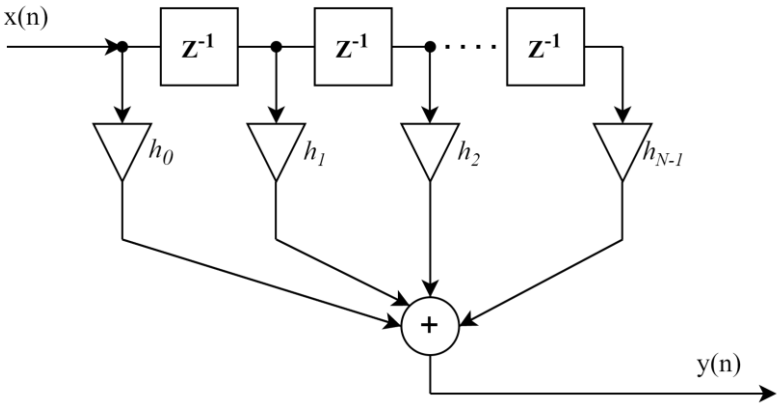


Рис. 1. Структурна схема трансверсального фільтру.

Рішенням показаного недоліку відомого підходу, може бути застосування адаптивного фільтру, якій крім декореляції сигналу від пасивної завади ще мінімізує енергію шуму [4]. Такий адаптивний фільтр з скінченною імпульсною характеристикою показано на рис. 2.

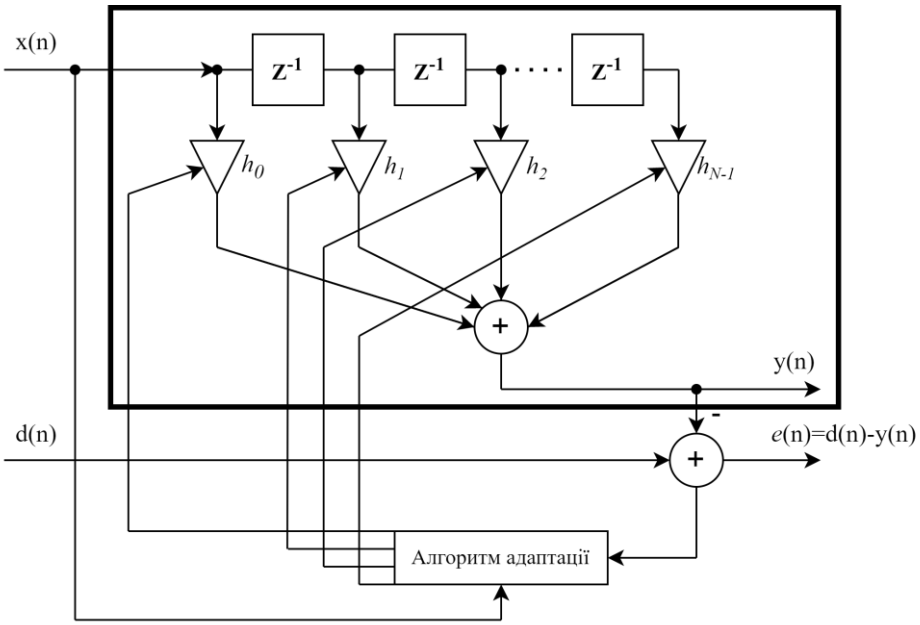


Рис. 2. Структурна схема адаптивного трансверсального фільтру придушення пасивної завади та зменшення потужності шуму.

На схемі фільтру, h_i - вагові коефіцієнти, z^{-1} - затримка сигналів на інтервал T - період випромінювання зондуючого сигналу РЛС. Сигнал $x(n)$ містить дві складові: сигнал від пасивної завади, і шумову складову. Фільтр повинен мати таку передаточну функцію, що забезпечує на виході сигнал у вигляді білого шуму з мінімальною потужністю. Для цього еталонний сигнал d(n), відносно якого визначається величина помилки $e(n) = d(n) - y(n)$, буде відображати дискретне значення теплового шуму [1]

$$d(t) = k_Б T_0 K_ш F \qquad (2)$$

де $k_Б$ - стала Больцмана, T_0 - температура оточуючого середовища 290 К, $K_ш$ - коефіцієнт шуму апаратури обробки сигналів 2-3 дБ, F - ширина спектру шуму, як правило для цифрової техніки $F = \frac{f_s}{2}$, f_s – частота дискретизації сигналу.

В результаті адаптації, фільтр забезпечує оптимальну обробку вхідного сигналу від пасивної завади, змішаного з адитивним шумом, за критерієм мінімуму середньоквадратичної помилки – мінімальна потужність [4]

$$\min J_{MSE} = \min M\{e^2(n)\}. \qquad (3)$$

Процес адаптації необхідно повторювати у відповідності до зміни завадо-об’єктної обстановки. При появі нових сигналів, відбитих від пасивних завад, або суттєвих змін характеристик уже відомих.

Висновок. Застосування адаптивного трансверсального фільтру з попереднім налаштуванням забезпечить ефективне виявлення БПЛА з малою ЕПР та швидкістю на фоні місцевих предметів, які формують сигнали пасивних завад роботі радіолокаційним системам.

Література

1. Теорія радіолокаційних систем (видання друге):підручник/ Б.Ф. Бондаренко, В.В. Вишнівський, В.П. Долгушин та іню; за заг.ред. С.В. Лєнкова. – К. Видавничо-поліграфічний центр «Київський університет», 2011.- 383с.
2. Основи теорії радіотехнічних систем: Навч. посібник. – Львів: Видавництво Національного Університету Львівська політехніка, 2005. 240 с.:іл. ISBN 966-553-439-4.
3. Методи та засоби обробки сигналів. Навчальний посібник./ Г. Д. Братченко, Б. В. Перелигін , О. В. Банзак, Н. Ф. Казакова, Д. В. Григор’єв — Одеса: Типографія-видавництво «Плутон», 2014. — 452 с.
4. Фактор часу в критичних режимах функціонування радіоелектронних систем./ Бичковський В.О.,Реутська Ю.Ю., Чмельов В.О. - Вісник НТУУ «КПІ». Серія Радіотехніка. Радіоапаратобудування . – К.: КПІ, 2018. – Вип. 75. – с. 25-32. DOI: https://doi.org/10.20535/RADAP.2018.75.25-32.

УДК 520.6.05

КРИТЕРІЇ ВИБОРУ АЛГОРИТМІВ КЕРУВАННЯ ПОТОКАМИ ІНФОРМАЦІЙНИХ ПОВІДОМЛЕНЬ СЕНСОРНИХ МЕРЕЖ

Явіся В.С., Лисенко О.І., Гетьман О.В.
Навчально науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: yavisya42@gmail.com

CRITERIA FOR THE SELECTION OF ALGORITHMS FOR CONTROLLING INFORMATION FLOWS OF SENSOR NETWORKS

The routing process has a significant impact on the efficiency, reliability and quality of the sensor network. Currently, there is no clearly defined approach to such a procedure. Of course, the choice of a specific routing algorithm should be made based on the results of their comparison according to certain indicators, which should take into account the technical, economic and quality requirements for the network.

Для підвищення ефективності та надійності функціонування сенсорних мереж необхідно вирішувати задачі керування трафіком. Процес керування трафіком можна розділити на наступні: прогнозування характеру та обсягу інформаційного трафіку в системі управління; визначення порядку доступу до мережних ресурсів, надання послуг зв’язку, показників і критеріїв якості обміну даними, порядку їх контролю; здійснення оперативного управління обміном даними для забезпечення необхідного рівня якості послуг зв’язку [1].

Процес маршрутизації має істотний вплив на ефективність, надійність та якість роботи сенсорної мережі. Тому вибір алгоритму маршрутизації повинен бути обґрунтованим та зваженим. На даний час відсутній чітко визначений підхід до такої процедури. Звичайно, що вибір конкретного алгоритму маршрутизації повинен здійснюватись за результатами їх порівняння по визначених показниках, які повинні враховувати технічні, економічні та якісні вимоги до мережі в цілому [2].

Вибір алгоритму маршрутизації в значній мірі залежить від наступних факторів, які можна вважати вихідними даними для процедури вибору.

• Топологія і складність мережі.

Необхідно передбачити наявність резервних ліній зв'язку в мережі, що забезпечують її надійне функціонування (доступність серверів і мережевих сегментів) у випадку відмов мережевого обладнання та основних ліній зв'язку.

• Розміри мережі та необхідність у її подальшому масштабуванні.

Можливості деяких протоколів в цьому сенсі обмежені.

• Завантаженість мережі.

Для мереж з високим коефіцієнтом завантаженості ліній зв'язку має значення здатність протоколу до перерозподілу потоків даних.

• Вимоги до надійності мережі.

Допустимий час простоїв або нестабільності в роботі мережі через відмови її вузлів залежить від роду діяльності організації, і визначається можливими фінансовими збитками або небезпекою порушення контролю та управління.

• Вимоги до захисту інформації в мережі.

Ці вимоги визначаються ступенем ризику, пов'язаного з потраплянням інформації про адреси та маршрути у мережі до рук зловмисників, що особливо важливо для мереж спеціального призначення.

• Необхідність підключення сегмента до вже існуючої мережі.

У цьому випадку слід звернути увагу на сумісність протоколів маршрутизації і засобів їх реалізації.

• Можливість організації програмних маршрутизаторів.

При невеликому трафіку в мережі або на окремих її ділянках від маршрутизаторів не потрібна висока продуктивність. У таких випадках з економічної точки зору буває вигідніше використовувати замість апаратного маршрутизатора універсальний комп'ютер з декількома мережевими картами та програмним забезпеченням (ПЗ), що реалізує функції протоколів маршрутизації. Проте не для всіх протоколів маршрутизації є відповідне ПЗ, а від складності протоколів залежить потужність обчислювальних ресурсів комп'ютера.

Виходячи з цього для порівняння протоколів маршрутизації пропонується обрати такі критерії:

• Швидкість збіжності.

Ця характеристика протоколу визначає тривалість часового інтервалу можливої нестабільної роботи мережі, в перебігу якого протокол виявляє недоступний маршрут, вибирає новий маршрут і розповсюджує нову інформацію по мережі. Швидкість реакції на зміни в мережевій топології особливо важлива при підтримці важливих додатків, які вимагають високого ступеня готовності мережі.

• Можливість обліку в метриці (критерії) вибору найбільш раціонального маршруту різних характеристик маршруту.

Метрики можуть розраховуватися на основі однієї або декількох характеристик шляху, до яких відносяться: кількість переходів (проміжних маршрутизаторів в дорозі); пропускна спроможність каналів зв'язку; затримка пакета в дорозі; надійність (частота виникнення помилок каналах зв'язку); навантаження (завантаженість маршрутизаторів і каналів зв'язку); вартість. Метрики, обчислені на основі декількох показників, забезпечують більшу гнучкість при виборі маршруту. Можливості протоколу підтримувати водночас декілька метрик дозволяють задовольняти вимоги QoS-трафіку (Quality of Service) різних додатків.

• Можливість балансування навантаження між декількома маршрутами.

Можливість зберігання в таблицях маршрутизації декількох маршрутів до однієї мережі (з рівними або навіть різними метриками) дає можливість маршрутизатору знижувати завантаження ліній зв'язку, шляхом почергового відсилання пакетів по кожному з маршрутів.

• Можливість об'єднання маршрутів на співпадаючих ділянках.

Наявність даної функції сприяє зниженню відносної складності великої мережі, скороченню кількості записів у таблицях маршрутизаторів і прискоренню пошуку в них. Об'єднання маршрутів вимагає, щоб протокол маршрутизації підтримував маски під мереж змінної довжини і був здатний поширювати інформацію про мережеві маски разом з інформацією про мережеві маршрути.

• Максимальна кількість маршрутизаторів в мережі визначає можливості її масштабування.

Це обмеження побічно пов'язане з іншими характеристиками протоколу маршрутизації, що впливають на його здатність працювати у великій мережі (наприклад, швидкістю збіжності, часткою смуги пропускання мережі, необхідної для передачі службових повідомлень протоколу).

• Необхідність попередньої логічної підготовки мережі.

Деякі протоколи маршрутизації для досягнення відповідного рівня масштабування (зменшення споживання обчислювальних ресурсів маршрутизаторів і смуги пропускання мережі) мають на меті виділення в мережі логічних областей і зв'язків між ними. Впровадження таких протоколів може вимагати серйозної інженерної проробки проекту мережі (її топології та схеми адресації).

• Забезпечення безпеки при обміні маршрутною інформацією.

Якщо мережа підтримує обмін маршрутною інформацією між підмережами, з'єднаними глобальними зв'язками, то потрапляння такої інформації до рук зловмисників може становити загрозу безпеці мережі. У таких випадках підтримка протоколом маршрутизації методів аутентифікації джерела і шифрування маршрутної інформації набуває важливого значення.

• Доступність програмного забезпечення реалізації протоколу маршрутизації.

Проколи можуть бути відкритими і підтримуватися різними виробниками апаратних маршрутизаторів і ПЗ для універсальних комп’ютерів, а можуть бути закритими і реалізуватися лише певними компаніями.

Таким чином, вибір алгоритму маршрутизації може здійснюватись по результатах порівняння за запропонованими критеріями з урахуванням важливості кожного з них, а також залежно від обсягу службового трафіку та обсягу обчислювальних процедур, необхідних для реалізації протоколу.

Література

1. Вакуленко О.В., Явіся В.С. Управління трафіком в транспортній мережі зв’язку відомчого призначення на основі збору інформації про інтенсивність інформаційних потоків та їх прогнозування // VII Науково-технічна конференція «Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення». Збірник тез. – К.: ВІТІ ДУТ. – 2014. – С. 73-74.
2. Явіся В.С., Вакуленко О.В. Обґрунтування вимог та критеріїв вибору алгоритму маршрутизації // VII Науково-технічна конференція «Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення». Збірник тез. – К.: ВІТІ ДУТ. – 2014. – С. 193-194.

УДК 621.382

ПРОЦЕС ФУНКЦІОНУВАННЯ ПОВІТРЯНИХ РАДІОМЕРЕЖ ІЗ САМООРГАНІЗАЦІЄЮ FANET

[2]Фуртат С.О., [2]Фуртат О.В., [1]Гетьман О.В.
[1]*Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна;*
[2]*Таврійський національний університет імені В.І.Вернадського, Україна*
E-mail:furtatsergij@gmail.com, furtatlena@gmail.com, lgetman78@gmail.com

THE PROCESS OF FUNCTIONING OF AIR RADIO NETWORKS WITH FANET SELF-ORGANIZATION

For the effective operation of a self-organizing radio network, network nodes must quickly adapt to frequent topology changes and efficiently use limited network resources. In such conditions, it is impossible to ensure information exchange with the given quality without an effective network management system.

The most difficult problems that stand in the way of building an effective control system are: limited bandwidth of network communication channels, limited capacity of installed power carriers in UAVs, which leads to the need to limit the computing power of control boards and radio transmitters. One of the ways to solve these issues is to use an effective method of routing in a self-organizing radio network, which will use network and node resources as efficiently as possible to maintain a high ratio of delivered packets (Packet Delivery Ratio), a low level of packet delay (Packet Delay) and ensure the required QoS (Quality of Service) for a given network.

Відсутність постійної інфраструктури та децентралізованого управління - характерні риси радіомереж із самоорганізацією.

Характерними особливостями даних мереж (на відміну від мереж з стаціонарною інфраструктурою) є наступні ознаки:

1. Змінна кількість вузлів і площа покриття мережі. Кількість вузлів мережі може варіюватися від десятків до десятків або сотень тисяч вузлів. Залежно від кількості вузлів, потужності їх передавачів і використовуваних частот географічний простір покриття мережі може змінюватися в широких межах.

2. Мобільність і стаціонарність вузлів. Стаціонарні Ad Hoc мережі зберігають незмінність місця розташування вузлів, але припускають їх довільне включення в мережу і від’єднання з мережі. Мобільні радіомережі із самоорганізацією MANET (Mobile Ad Hoc Networks) передбачають можливість переміщення будь-якого вузла мережі.

3. Випадковість топології мережі, її неоднорідність і динамічність зміни. Оскільки абоненти мережі можуть бути мобільними, то топологія мережі може постійно змінюватися. Крім того, кожен вузол може мати різні радіо ресурси та обчислювальні потужності - мати різну потужність передавача, мати можливість змінювати рівень потужності передавача або діаграму спрямованості антени, бути оснащеним акумуляторними батареями різної ємності.

4. Принцип організації передачі інформації - комутація пакетів з використанням багатокрокової маршрутизації. Цей принцип полягає в тому, що кожен вузол мережі, будучи передавачем і приймачем "власної" інформації, виступає в якості ретранслятора і маршрутизатора пакетів інших абонентів мережі. Під маршрутизацією розуміється направлення пакетів на певні адреси або ретрансляція сигналів в певних напрямках.

5. Децентралізований тип управління. Таке управління передбачає автономність вузлів в прийнятті рішень по організації передачі за визначеними маршрутами. Іншими словами, в мережі відсутня будь-яка фіксована інфраструктура для передачі службової інформації чи іншого виду централізованого управління (на відміну від звичайних телекомунікаційних мереж з системами управління [3,4]). Кожен вузол визначає маршрут передачі - послідовність вузлів-ретрансляторів на основі попереднього або оперативного збору інформації про стан мережі і зв'язності її абонентів відповідно до протоколів маршрутизації, спеціально розробленими для мереж із самоорганізацією.

6. Динамічність зміни зв'язності при пересуванні вузлів і / або приєднання / від’єднання вузлів в мережу. Це вимагає контролю за проходженням пакетів по мережі, зміни маршрутів пакетів при порушеній зв'язності, а також відновлення передачі повідомлень з моменту втрати зв'язності. Такий характер роботи мереж призводить до зміни якості обслуговування мережею (затримка і втрата пакетів, повна втрата зв'язності). Тому в мережах із самоорганізацією повинні бути передбачені механізми підтримки якості обслуговування за рахунок, наприклад, передачі пакетів по декільком маршрутам, колективної ретрансляції пакетів.

7. Багатоканальність мереж. Кожен вузол може бути обладнаний одним або декількома приймально-передавальними пристроями, що працюють в різних частотних смугах. Таким чином, крім комутації пакетів в одному частотному каналі можлива комутація каналів.

8. Масштабованість. При масштабованості мережа легко збільшується і змінює кількість своїх вузлів. Збільшення розміру мережі до сотень і тисяч вузлів може вимагати введення локалізації управління, тобто поділ всієї

мережі на кластери з власними протоколами маршрутизації і міжкластерною ретрансляцією через вузли-шлюзи. Можливо і введення ієрархії в мережі, коли на основі вузлів, що мають достатні ресурси або гарне місце розташування (наприклад, на вершинах пагорбів), здійснюється прямий зв'язок між кінцевими абонентами або кластерами через мінімальну кількість ретрансляцій.

9. Обмеженість ресурсів вузлів мережі. Вузол мережі має обмежені ресурси (ємність пам'яті, продуктивність процесора, потужність передавача і енергоємність батарей). Енергія батарей витрачається як на комунікаційну (прийом, передача, обробка повідомлень і ін.), так і на обчислювальну (процесор) складові. Економія енергії батарей живлення - одне із завдань розробників терміналів і протоколів взаємодії.

10. Обмежена безпека. Широкомовна природа радіоканалу дозволяє зловмиснику (противнику) здійснювати прослуховування передач вузлів, аналізувати мережевий трафік і порушувати або погіршувати роботу мережі, ставити активні і пасивні перешкоди. Тому в мережі повинні бути вжиті заходи, які мінімізують або виключають можливий навмисний негативний вплив на роботу мережі. Таким заходом може бути застосування на фізичному рівні складних радіосигналів, наприклад надширокосмугових.

Розвиток елементної бази і більші обчислювальні потужності на сьогоднішній день визначили різноманіття радіомереж із самоорганізацією (рис.1):

- мережі Ad Hoc - мережі з випадковими, але стаціонарними абонентами;

- мобільні радіомережі (мережі MANET) - мережі мобільних абонентів, які реалізують повністю децентралізоване управління (відсутність базових станцій);

- mesh мережі (MESH) - такі мережі складаються з бездротових стаціонарних маршрутизаторів (створюють бездротову магістраль і зону обслуговування абонентів) і мобільних / стаціонарних абонентів, що мають доступ (в межах зони радіозв'язку) до одного з маршрутизаторів;

- сенсорні (телеметричні) мережі, що складаються з малогабаритних сенсорних вузлів з інтегрованими функціями моніторингу певних параметрів навколишнього середовища, обробки і передачі даних по радіоканалах;

- автомобільні мережі (мережі VANET) - мережі зв'язку транспортних засобів.

- Повітряні мережі (мережі FANET) - мережі на основі БПЛА.

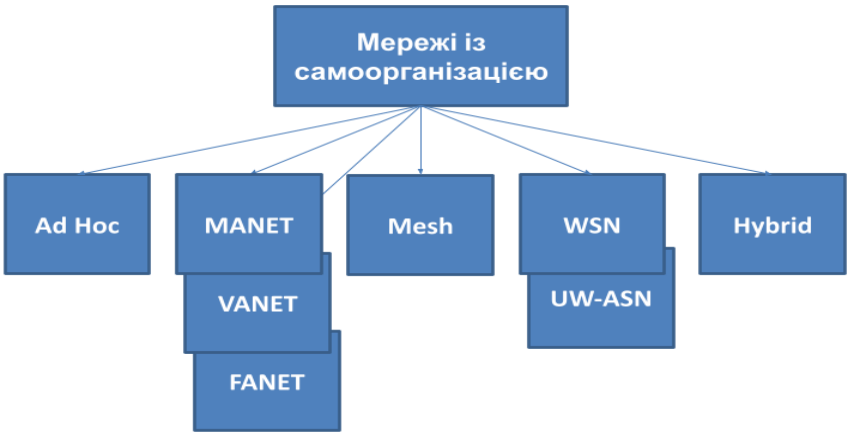


Рис.1. Класифікація мереж із самоорганізацією.

Переваги мереж із самоорганізацією очевидні: відсутність етапу планування (можливість самоорганізації), швидке розгортання, децентралізоване управління (дуже висока живучість), робота в русі всіх елементів мережі .

Література

1. Kahn R. Advances in Packet Radio Technology // Proc, of the IEEE. — 1978. - 66. — P. 1468-1496.
2. Бунин С.Г, Войтер А.П. Вычислительные сети с пакетной радиосвязью. — К.: Техніка, 1989. - 223 с.
3. Эфремидес Э., Уизелтир Д.Э., Бейкер Д.Д. Вопросы проектирования надежных мобильных радиосетей, использующих методы передачи и приема сигналов с псевдослучайной перестройкой рабочей частоты // ТИИЭР. - 1987. - 75, № 1. - С. 68-90.
4. Fifer W., Bruno F. The Low-Cost Packet Radio // Proc, of the IEEE - 1987. — 75 (1). - P. 33-42.
5. Sharret IP. WIN-T-The Army's New Tactical Intranet // IEEE MILCOM. - 1999. - P. 45.04.01- 45.04.05.
6. Freebersyser J., Leiner B. A DoD Perspective on Mobile Ad Hoc Networks // Ad Hoc Networking. - 2001. - 25. - P. 147-152.
7. Sass P. Communications Networks for the Force XXI Digitized Battlefield // ACM/Baltzer Mobile Networks and Applications Journal. — 1999. — 4. — P 450—455.
8. Ramachandram K.N., Buddhikot M.M., Miller S. On design and implementation of infrastructure mesh networks // Proc, of WiMesh'05. - 2005. - P. 785-790.
9. Salem N.B., Hubaux J.-P. Securing Wireless Mesh Networks // IEEE Wireless Communications. - 2006. - 13, N 2. - P. 625-631.

УДК 621.382

МЕТОДИКА ПОБУДОВИ ЗАХИЩЕНОЇ МЕРЕЖІ НА ОСНОВІ ОБЛАДНАННЯ JUNIPER

Валуйський С.В., Кравчук І.В.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: ilyukha.kravchuk@gmail.com

METHODOLOGY FOR BUILDING A SECURE NETWORK BASED ON JUNIPER EQUIPMENT

This article examines the possibility of building a secure and fault-tolerant network based on Juniper routers, with particular attention given to the LACP, VPN, RSTP, and TAP protocols. Their main advantages in network usage are identified.

Компанія Juniper вважається однією із провідних постачальників у світі. Вона була заснована о 1996 році і з того часу вона стала однією з провідних компаній у галузі мережевого обладнання. Тенденція її популярності змінювалася залежно від ринкових умов та конкуренції, проте загалом компанія зберегла свою популярність серед клієнтів, що шукають високоякісне та надійне мережеве обладнання.

У 2022 році аналітична компанія 650 Group дослідила та встановила, що протягом I кварталу 2022 року продаж технологій Juniper Mist AI збільшився на 117 %, що має найвищий відсоток росту прибутку в порівнянні з іншими конкурентами виробників засобів безпровідного зв’язку [1].

Мета роботи. Побудувати захищену та відмовостійку мережу на основі обладнання Juniper. Для забезпечення відмовостійкості буде використано протоколи LACP та RSTP. Для захисту мережі будуть використане налаштування VPN, TAP, а також стандартних профілів безпеки як ACL. Топологія цієї мережі буде побудована у вигляді кільця, буде використана віртуальна лабораторія GNS3 з використанням віртуального образу Juniper router, PC, а також додаткових комутаторів від вендора Cisco.

Властивості та призначення протоколів, які будуть використанні в роботі.

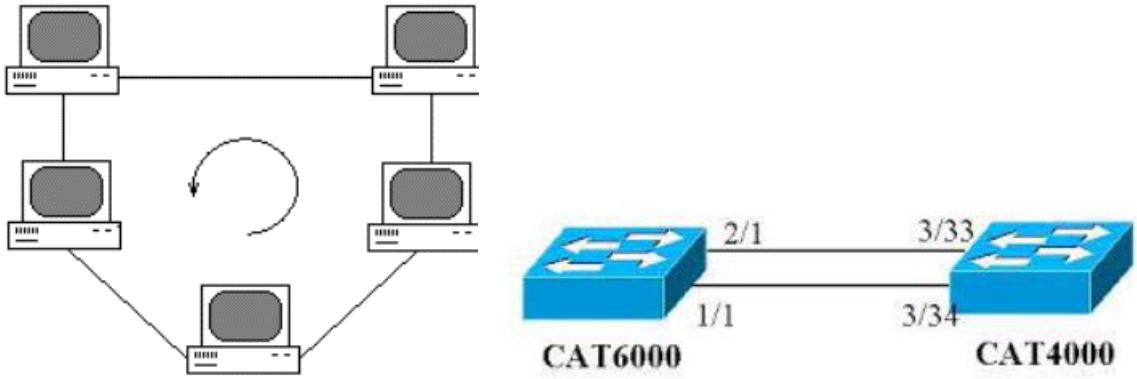
LACP – це протокол керування з'єднаннями, який використовується для об'єднання між собою кількох мережевих портів в один логічний канал, який називається Link Aggregation Group (LAG). LACP забезпечує створення та управління LAG між двома мережевими пристроями, зокрема між

комутаторами, маршрутизаторами, серверами, забезпечуючи збільшення швидкості передачі даних, збільшення надійності та забезпечення балансування навантаження [2].

RSTP (Rapid Spanning Tree Protocol) є протоколом, який використовується для запобігання петель у мережах з топологією дерева. Цей протокол є удосконаленням протоколу Spanning Tree Protocol (STP), який був розроблений для запобігання петель у мережах з топологією дерева. RSTP відповідає за визначення шляху, який буде використовуватися для передачі даних в мережі. Він також забезпечує автоматичну реакцію на зміни топології мережі, що дозволяє мережі бути більш масштабованою та надійною [3].

Налаштування політик безпеки для пропуску або відкидання трафіку – це процес налаштування правил та налаштувань в мережному обладнанні або програмному забезпеченні, які визначають, який трафік мережі повинен бути дозволений для проходження, а який повинен бути заблокований чи відкинутий. У Juniper налаштування політик безпеки для пропуску або відкидання трафіку зазвичай здійснюється за допомогою механізму Juniper Security Policies [4].

TAP – це тип мережевого інтерфейсу, який дозволяє передавати дані між комп'ютерами на різних рівнях мережевої моделі OSI. У контексті VPN, TAP використовується для передачі Ethernet-кадрів через тунель між двома або більше комп'ютерами, що знаходяться на різних кінцях VPN-підключення. Застосування TAP-адаптера у VPN дозволяє розширити мережевий доступ між комп'ютерами на різних фізичних мережах через інтернет-підключення [5].



а) б)

Рис. 1. Тологія «кільце» (а) та приклад використання LACP (б).

На Рис.1б представлений приклад використання протоколу LACP. Якщо щось станеться з фізичним каналом 2/1 – 3/33, то мережа буде далі функціонувати, так як канал фізичний канал 1/1 – 3/34 буде далі працювати і навпаки. Цей протокол не тільки підвищує відмовостійкість мережі, а й збільшує її пропускну здатність. Тобто два фізичних каналу утворюють один логічний з вищою пропускною здатністю та відмовостійкістю.

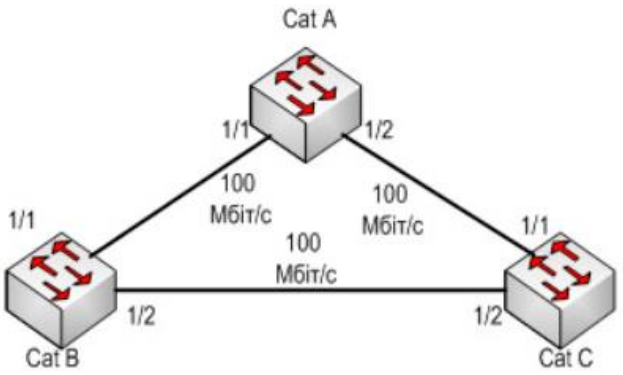


Рис. 2. Приклад використання RSTP.

На рис.2 представлене використання протоколу RSTP. Інтерфейси 1/2-1/2 між CatB – CatC знаходять у режимі DOWN, в той час як інтерфейси 1/1-1/1 між CatB – CatA та інтерфейси 1/2-1/1 між CatA – CatC знаходяться в режимі FRW. Якщо щось станеться наприклад з CatA, то вся мережа не впаде, а піднімуться інтерфейси 1/2-1/2 між CatB – CatC (перейдуть в режим FRW), тоді трафік зможе передаватись між ними.

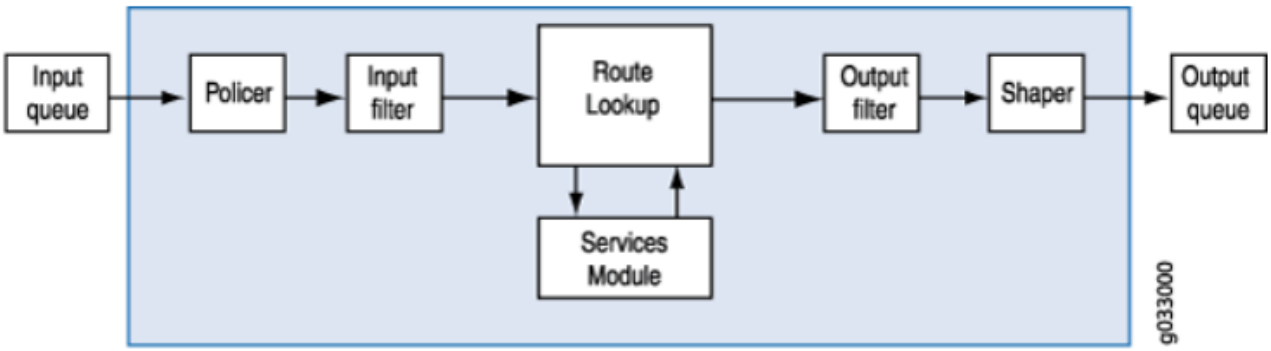


Рис. 3. Принцип роботи політик безпеки та протоколу TAP.

Як можемо бачити на рис.3, коли пакети надходять на пристрій, до них застосовуються класифікатори, фільтри та захисники. Далі визначається

інтерфейс джерела пакета, виконавши пошук маршруту. Коли вихідний інтерфейс для пакета знайдено, застосовується фільтр, і пакет надсилається до вихідного інтерфейсу, де він ставиться в чергу та запланований для передачі. Пересилання на основі пакетів не потребує жодної інформації про попередній чи наступний пакет, що належить даному з'єднанню, будь-яке рішення щодо дозволу чи заборони трафіку залежить від пакету. Ця архітектура має перевагу масового масштабування, оскільки вона пересилає пакети без відстеження окремих потоків або станів.

Висновок. Отже враховуючи всі вище перераховані протоколи, техніки та особливості обладнання Juniper з його операційною системою Junos, можна побудувати захищену мережу від стороннього проникнення, а також бути впевненим, що у випадку непередбачуваних ситуацій мережа буде в робочому стані.

Література

1. Juniper Networks is recognized as a leading manufacturer of corporate and wireless local area networks. URL: https://itbiz.ua/news/kompaniya-juniper-networks-viznana-providnim-virobnikom-korporativnix-ta-bezprovidnix-lokalnix-merezh/ (the date of access: 24.03.2023).
2. 802.1AX-2020 - IEEE Standard for Local and Metropolitan Area Networks--Link Aggregation. URL: https://ieeexplore.ieee.org/document/9105034 (the date of access: 24.03.2023).
3. Understand Rapid Spanning Tree Protocol (802.1w) URL: https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24062-146.html (the date of access: 24.03.2023).
4. Security Policies User Guide for Security Devices URL: https://www.juniper.net/documentation/us/en/software/junos/security-policies/topics/topic-map/security-policy-configuration.html (the date of access: 24.03.2023).
5. Flow-Based and Packet-Based Processing User Guide for Security Devices URL: https://www.juniper.net/documentation/us/en/software/junos/flow-packet-processing/topics/topic-map/security-tap-mode-flow.html (the date of access: 24.03.2023).

УДК 621.382

АНАЛІЗ ФУНКЦІОНУВАННЯ ПРОТОКОЛУ OPENFLOW В ЛОКАЛЬНИХ МЕРЕЖАХ

Валуйський С.В., Гірук Д.О.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: dianahiruk@gmail.com

ANALYSIS OF THE OPERATION OF THE OPENFLOW PROTOCOL IN LOCAL NETWORKS

This article discusses the transition beyond the traditional network infrastructure, namely the possibility of making it a dynamic network using SDN software. The implementation of the OpenFlow protocol and architecture in SDN is considered in detail. The integration, advantages and problems of the OpenFlow protocol in a local network are analyzed.

Завдяки швидкому розвитку інформаційних технологій та появі нових технологій, таких як хмарні обчислення та великі дані, вимоги до комп'ютерних мереж стають все більш складними. Для забезпечення високої швидкості передачі даних та ефективного управління мережами виникають нові технології з ускладненою інфраструктурою, що потребують вдосконалення інструментів моніторингу і управління.

Одним зі засобів вирішення цих проблем є використання програмно-конфігурованих мереж SDN (Software-Defined Networks). Ця технологія пропонує нові реалізації, які дозволяють вирішувати більше завдань та забезпечувати більш ефективне управління мережами, зокрема через використання протоколу OpenFlow. Ідея мереж SDN вже присутня понад десять років, але недавні реалізації відомих компаній відкривають нові можливості її використання [1].

Мета роботи. Основна мета роботи полягає в аналізі переваг протоколу Open-Flow у традиційному середовищі локальної мережі та його інтеграції та сумісності з деякими популярними протоколами в локальній мережі, наприклад, віртуальними локальними мережами (VLAN).

Інтеграція, переваги та проблеми протоколу OpenFlow у локальній мережі.

OpenFlow – це відкритий стандарт, який пропонує програмне керування мережевим обладнанням. Спочатку він був розроблений для дослідників мереж, щоб перевірити свої експериментальні протоколи на реальних мережевих апаратних пристроях і мережах кампусів, які представляють повсякденне мережеве середовище, наприклад LAN і WAN. Спільнота

дослідників мереж стикається з надзвичайно високими перешкодами для експериментування нових ідей або протоколів у виробничому або традиційному мережевому середовищі. Для того, щоб використовувати доступне мережеве обладнання та розгорнуту мережу для тестування експериментальних протоколів і нових ідей, наприкінці 2008 року з'явився

OpenFlow, а в грудні 2008 року випустив свої перші специфікації [2]. У існуючій інфраструктурі мережеві пристрої приймають рішення на рівні мережі, такі як маршрутизація або доступ до мережі. Існує багато комерційних постачальників мережевих пристроїв, які використовують різні мікропрограми у своїх пристроях, і мережа зазвичай налаштована у відкритому режимі, а не за пропрієтарним способом для підтримки пристроїв від різних постачальників. Відкритий мод означає розгортання, незалежне від постачальника, а пропрієтарний — розгортання, що залежить від постачальника, і розгортається часто. Залежно від постачальника та його мережевого пристрою було важко перевірити нові дослідницькі ідеї, такі як протоколи маршрутизації, і встановити їх сумісність у реальних мережах. Крім того, спроба будь-яких експериментальних ідей над виробничою мережею з критичним

пріоритетом може призвести до збою мережі в якийсь момент, що призвело до статичності та негнучкості мережевої інфраструктури та не привернуло серйозних інновацій у цьому напрямку [3].

Таблиці пошуку в комутаторах і маршрутизаторах Ethernet були основним ключем для впровадження брандмауерів, NAT, QoS або збору статистики продуктивності. OpenFlow враховує загальний набір функцій, що підтримується більшістю постачальників, що допомагає досягти стандартного способу використання таблиць потоків для всіх мережевих пристроїв, незалежно від їх постачальника. Це дозволяє розділити мережу на основі потоку, організовуючи мережевий трафік у різні класи потоків, які можна згрупувати разом або ізольувати для обробки, маршрутизації або контролю в бажаний спосіб. OpenFlow можна широко використовувати в кампусних мережах, де ізоляція дослідницького та виробничого трафіку є однією з найважливіших функцій.

У мережевих пристроях існує три площини: площина даних, площина управління, однак в цій роботі зосереджені лише дані та площина керування. У SoftRouter була запропонована подібна архітектура, яка підкреслює роз'єднання даних і площини керування, спрямована на забезпечення більш ефективного пересилання пакетів [4]. OpenFlow нагадує ці архітектури в

концепції поділу даних і площини керування, але підтверджує концепцію обробки на основі потоку за допомогою таблиць потоку. Потоки мають бути ретельно налаштовані, оскільки невідповідність призводить до пересилання пакетів до контролера OpenFlow, який може прийняти рішення про трансляцію пакетів, і призведе до різкого зниження пропускної здатності з 941 Мбіт/с до приблизно 340 Кбіт/с у гігабітній мережі.

Щоб отримати програмований контроль над площиною керування, потрібні
комутатори, що підтримують OpenFlow, і контролер, що містить мережеву логіку. OpenFlow базується на комутаційному пристрої з внутрішньою таблицею потоків і забезпечує відкриту програмовану віртуалізовану комутаційну платформу для керування обладнанням комутатора за допомогою програмного забезпечення. Він може реалізовувати функцію комутатора, маршрутизатора або навіть обох, і дозволяє програмно керувати шляхом керування мережевим пристроєм через протокол OpenFlow.

З'єднання контролера OpenFlow захищено здебільшого за допомогою SSL або TLS, але воно може бути вразливим до атак на відмову в обслуговуванні (DoS); тому для запобігання таким атакам необхідновжити суворих заходів безпеки. В архітектурі OpenFlow перенаправлення потоку даних все ще знаходиться на комутаторі, але рішення про перенаправлення потоку приймаються в окремому контролері OpenFlow або ієрархії контролерів, яка реалізована на сервері (серверах), які спілкуються з комутаторами з підтримкою OpenFlow у мережі через протокол OpenFlow.

Таким чином, основними компонентами мережі OpenFlow є:

- комутатори з підтримкою OpenFlow
- сервер(и), на яких працює контролер(и).

Щоб керувати динамічною мережею, можна розробити структуру автоматизації, яка відповідно додає або видаляє потоки. Концепцію потоку можна інтерпретувати як уникання маршрутизаторів у мережі, але насправді потоки не перекривають функції маршрутизатора [5].

Повну інтеграцію з локальними мережами не вдасться досягти через відсутність підтримки протоколів рівня 3 і повільну інтеграцію OpenFlow в апаратне забезпечення. Протокол OpenFlow більше підходить для центрів обробки даних або магістральних мереж для обробки зростаючих даних, а також для невеликих мереж, таких як мережі кампусу, для ізоляції дослідницького трафіку від мережевого.

Найголовнішою перевагою протоколу можна вважати незалежне та програмоване керування мережею.

Також можна виділити ще деякі з переваг протоколу OpenFlow:

- Простота управління мережею: OpenFlow дозволяє розгортання та керування мережею з одного місця. Це дає змогу швидко реагувати на зміни в мережі та забезпечує більш ефективне використання ресурсів.
- Гнучкість: OpenFlow дозволяє створювати власні правила для керування потоками даних. Це дає змогу використовувати мережу для різних цілей та забезпечує більш ефективне використання ресурсів.
- Зменшення витрат на обладнання: OpenFlow дозволяє використовувати дешевіші комутатори замість дорогих традиційних комутаторів, що дає змогу зменшити витрати на обладнання.
- Більша безпека: OpenFlow дозволяє розгортати більш ефективні системи безпеки, що забезпечують захист від атак з мережі.
- Більша масштабованість: OpenFlow дозволяє створювати більш складні мережі, що мають більшу масштабованість та ефективність, порівняно з традиційними мережами [6].

Висновок. Протокол OpenFlow дозволяє ефективно керувати мережею та забезпечує більшу гнучкість та безпеку в порівнянні з традиційними мережами.

Література

1. "Software-Defined Networking (SDN) Definition" від Open Networking Foundation - https://www.opennetworking.org/sdn-resources/sdn-definition/
2. Trema. [www]. [Cited 6.5.13]. Available at: https://github.com/trema/trema
3. Dietz, T. Trema Tutorial. [www]. [Cited 6.5.13]. Available at: http://www.fp7-ofelia.eu/assets/Uploads/201203xx-TremaTutorial.pdf
4. T.V. Lakshman, T. N. (2004). The SoftRouter Architecture. SIGCOMM Hot Topics in Networks III (HotNets III) workshop. San Diego, CA.
5. Casado, M., & Pettit, J. (2011). OpenFlow in the enterprise: A practical use case. ACM SIGCOMM Computer Communication Review, 41(5), 34-41.
6. Open Networking Foundation. (2021). OpenFlow Switch Specification, Version 1.5.1. Retrieved from https://www.opennetworking.org/wp-content/uploads/2014/10/openflow-switch-v1.5.1.pdf

УДК 621.382

АЛГОРИТМ РОЗГОРТАННЯ ШЛЮЗІВ ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ РОЗУМНОГО ДОМУ

Валуйський С. В., Пономаренко І. О.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: valuiskyi.stanislav@lll.kpi.ua

ALGORITHM OF IOT GATEWAY DEPLOYMENT FOR SMART HOME

This article examines a method for deploying IoT gateways in smart homes using optimization models. The models aim to determine the minimum number of IoT gateways required to cover a desired area, their locations, and the distribution of IoT devices to the corresponding gateways. The study considers communication technologies such as ZigBee, Wi-Fi, and BLE and uses linear programming to optimize the number of gateways and devices.

Інформаційні технології стали невід'ємною частиною повсякденного життя людей та підприємств, а концепція Інтернету речей (IoT) безпосередньо сприяє змінам у повсякденному житті. У зв'язку зі зростанням популярності розумних будинків, планування та оптимізація розгортання шлюзів Інтернету речей (IoT) стає все більш актуальною проблемою. Шлюзи IoT відіграють ключову роль у забезпеченні ефективної комунікації між пристроями в розумному будинку. На сьогодні не достатньо вирішеною є проблема планування та оптимізації розгортання шлюзів у розумних будинках, а саме проблема мінімізації кількості шлюзів розумного будинку та розгортання мінімальної кількості шлюзів, щоб кількість розгорнутих шлюзів для підтримки зв’язку пристроїв Інтернету речей могла бути мінімізована.

Математична постановка задачі. Враховуючи мету мінімізації кількості шлюзів, визначимо змінні для прийняття рішення:

$X_{i,j}$ – матриця зв'язків між пристрями із шлюзом;

Y_i – множина шлюзів, які були активовані для задоволення потреб пристроїв.

У таблиці 1 представлені параметри, які були використані для моделі оптимізації, заснованої на лінійному програмуванні. Враховуючи координати пристроїв Інтернету речей ($D_{i,j}$), оптимізаційна модель передбачала з'вязок коженого пристрою із шлюзом (Y_i). Шлюз повинен бути в межах досяжності певної радіо технології (r). Цей зв'язок відбувся за допомогою змінних прийняття рішення. Кожному пристрою було призначено шлюз, але з кожним певним шлюзом могло бути пов'язано декілька пристроїв. Модель використовувала ці обмеження для створення асоціацій, які відповідали необхідним критеріям для досягнення запропонованої мети. Мета оптимізаційної моделі представлена рівнянням (1):

$$\boldsymbol{min \sum_{i=1}^{n} Y_i} \qquad \textbf{(1)}$$

де Y_i представляє активні шлюзи. Рівняння (1) являє собою мінімізацію кількості шлюзів (Y_i). Кожен $D_{i,j}$ є точкою-кандидатом на шлюз.

Таблиця 1. Змінні в моделі оптимізації лінійного програмування.

Змінна	**Опис**
r	Діапазон безпроводової технологій
n	Кількість розгорнутих пристроїв
c	Смуга пропускання, яка використовується пристроєм
cb	Загальна пропускна здатність каналу зв'язку
$\boldsymbol{A_{i,j}}$	Всі можливі точки в межах бажаної області
$\boldsymbol{D_{i,j}}$	Координати розгорнутих пристроїв
$\boldsymbol{Mdist_{i,j}}$	Матриця відстані (вимірюється між точкою пристрою та точками інших розгорнутих пристроїв)
$\boldsymbol{Mativ_{i,j}}$	Двійкова матриця (де 0 вказує на те, що відстань між пристроями не знаходиться в межах досяжності, а 1 вказує на те, що відстань між пристроями знаходиться в межах досяжності технології)

Визначимо мінімальну кількість шлюзів, необхідну для забезпечення покриття пристроїв Інтернету речей:

$$\sum_{j=1}^{n} X_{i,j} = 1, \qquad i = 1, \dots, n \tag{2}$$

$$X_{i,j} \leq Mativ_{i,j} * Y_i, \qquad i, j = 1, \dots, n \tag{3}$$

$$\sum_{j=1}^{n} X_{i,j} = 1 * c - cb \leq 0 \tag{4}$$

$$X_{i,j} \geq 0, \qquad i, j = 1, \dots, n \tag{5}$$

$$Y_i \geq 0, \qquad i, j = 1, \dots, n \tag{6}$$

Обмеження, які спричинені рівняннями (2) та (3), мають на меті зв'язати пристрій з одним шлюзом. Рівняння (4) обмежує кількість пристроїв на шлюз з урахуванням пропускної здатності каналу зв'язку і не допускає перевищення певної максимальної пропускної здатності. У випадку, коли максимальна пропускна здатність буде перевищена, активується інший шлюз для задоволення необхідних вимог. Рівняння (5) та (6) створюють невід'ємні обмеження.

Реалізація оптимізаційної моделі дозволяє визначити активні шлюзи (Y_i) та асоціацій між пристроями та відповідними шлюзами ($X_{i,j}$). Виходячи з цих результатів, можна побудувати графік, використовуючи модель розумного дому або підприємства, на якому показати положення шлюзів і відповідних пристроїв Інтернету речей, утворюючи таким чином кластер.

Опис алгоритму. Планування та оптимізація розгортання шлюзу IoT для мереж зв'язку мають на меті розрахувати мінімальну кількість шлюзів, необхідних для покриття певної території, та кількість пристроїв IoT на шлюз. Для кількісної оцінки враховується діапазон використовуваної технології бездротового зв'язку і пропускна здатність каналу зв'язку шлюзу. Кінцевою метою було мінімізувати кількість шлюзів при максимальному охопленні пристроїв у межах бажаної зони.

Кожна пара координат для нанесених точок у певній області була використана як вхідний параметр для моделі оптимізації, заснованої на лінійному програмуванні. Запропонована модель передбачає вибір точки встановлення пристроїв IoT випадковим чином, використовуючи початкове значення, але вони також могли бути визначені відповідно до реальності їх розгортання (тобто їх реальних позицій). При використанні реальних позицій необхідно було мати координати місця, в якому повинно було бути розгорнуто пристрій.

Література

1. Planning and Optimization of Software-Defined and Virtualized IoT Gateway Deployment for Smart Campuses / D. Ferreira та ін. Sensors. 2022. Т. 22, № 13. С. 4710. URL: https://doi.org/10.3390/s22134710.
2. Efficient Gateways Placement for Internet of Things with QoS Constraints / I. Gravalos та ін. GLOBECOM 2016 - 2016 IEEE Global Communications Conference, м. Washington, DC, USA, 4–8 груд. 2016 р. 2016. URL: https://doi.org/10.1109/glocom.2016.7841780.

УДК 621.396.96

АДАПТИВНА ТРАЄКТОРНА ФІЛЬТРАЦІЯ МАЛОРОЗМІРНОГО БПЛА ПРИ КОМПЛЕКСНОМУ ВИКОРИСТАННІ ДАНИХ РЛС І ВІДЕОКАМЕРИ

Соколов К.А., Жук С.Я.
Радіотехнічний факультет КПІ ім. Ігоря Сікорського, Україна
E-mail:k.sokolov@kpi.ua, s.zhuk@kpi.ua

SMALL-SIZED UAVS ADAPTIVE TRAJECTORY FILTERING WITH COMPLEXING USE OF RADAR AND VIDEO CAMERA DATA

The article considers the problem statement and synthesis of the adaptive trajectory filtering algorithm for small-sized UAVs with the integrated use of radar and video camera data, and analyzes its performance measures

На сьогодні важливе значення має задача виявлення і супроводження малорозмірних безпілотних літальних апаратів (МБПЛА) [1]. Широкого використання для її вирішення знайшли РЛС і відеокамери, які часто застосовуються сумісно. Сучасні МБПЛА, відносяться до інтенсивно маневруючих об’єктів, які спроможні рухатись із значними перевантаженнями. Тому актуальною задачею є розробка адаптивних алгоритмів траєкторних фільтрації МБПЛА за даними РЛС і відеокамери.

Рух МБПЛА з різними видами маневру в прямокутній системі координат описується математичною моделлю у вигляді стохастичної динамічної системи з випадковою структурою в дискретному часі [2]:

$$\mathbf{u}(k) = \mathbf{B}_j \mathbf{u}(k-1) + \mathbf{C}_j \mathbf{w}(k), \ j = \overline{1, M}, \qquad 1)$$

де $\mathbf{u}(k)$ - вектор стану, що включає параметри руху МБПЛА по осях прямокутної місцевої СК; $\mathbf{w}(k)$ – некорельована послідовність гаусівських векторів $\mathbf{M}[\mathbf{w}(k)] = 0$, $\mathbf{M}[\mathbf{w}(k)\mathbf{w}^T(k)] = \mathbf{I}$; $\mathbf{F}_j$, $\mathbf{C}_j$ - відомі матриці.

Для керування зміною структури моделі (1), використовується ланцюг Маркова $a_j(k)$, $j = \overline{1, M}$ з відомими ймовірнісними характеристиками.

Враховуючи обмеження щодо обсягу матеріалу, розглянуто випадок одночасного отримання даних від РЛС і відеокамери. В якості РЛС використано FMCW-радар, який вимірює дальність $r^{\text{РЛС}}(k)$, радіальну швидкість $\dot{r}^{\text{РЛС}}(k)$, азимут $\beta^{\text{РЛС}}(k)$, кут місця $\varepsilon^{\text{РЛС}}(k)$ МБПЛА в сферичній СК, пов’язаній з місцем розташування РЛС. Відеокамера вимірює азимут $\beta^{\text{В}}(k)$, кут місця $\varepsilon^{\text{В}}(k)$ МБПЛА в сферичній СК, пов’язаній з її місцем розташування. Шляхом лінеарізації нелінійних рівнянь вимірювання параметрів руху МБПЛА в сферичних СК отримати лінійні рівняння вимірювання координат БПЛА в єдиній прямокутній СК

Розширений процес $(\mathbf{u}(k), a_j(k))$ належить до класу змішаних

марківських процесів у дискретному часі. Використовуючи метод синтезу оптимальних і квазіоптимальних алгоритмів оцінювання змішаних марківських процесів в дискретному часі [2], розроблено алгоритм адаптивної траєкторної фільтрації МБПЛА при комплексному використанні даних РЛС і відеокамери**.** Особливість синтезованого алгоритму полягає у нерозривній зв'язаності рівнянь фільтрації та екстраполяції дискретного $a_j(k)$ та неперервного $\mathbf{u}(k)$ компонентів між собою. При цьому апостеріорна щільність ймовірності $W(\mathbf{u}(k))$ неперервного компоненту при переході на наступний крок фільтрації апроксимується сумою M гаусівсьских щільностей ймовірності. Адаптивний фільтр містить M каналів і відноситься до класу пристроїв зі зворотними зв'язками між каналами. При отриманні данних лише від РЛС, розроблений алгоритм співпадає з наведеним в [3].

Аналіз точносних характеристик синтезованого алгоритму оцінювання параметрів руху МБПЛА з розпізнаванням різних видів руху виконано за допомогою статистичного моделювання на ЕОМ. Модель руху МБПЛА описується стохастичною динамічною системою з випадковою структурою (1), яка враховує три основних види руху $M = 3$: зависання $j = 1$, майже рівномірний рух $j = 2$, рух з маневром $j = 3$. Вектор стану має наступний вигляд (2)

$$\mathbf{u}^T(k) = (x(k), \dot{x}(k), \ddot{x}(k), y(k), \dot{y}(k), \ddot{y}(k), \mathrm{z}(k), \dot{\mathrm{z}}(k), \ddot{\mathrm{z}}(k)) \qquad 2)$$

Темп формування траєкторії БПЛА Т = 1 секунда. Для наочності аналізу ефективності роботи алгоритму тестова траєкторія була розбита на інтервали, на яких моделювався відповідний тип руху: $1 \le k \le 9-$ $j = 2$, $10 \le k \le 15$ $j = 3$, $16 \le k \le 20-$ $j = 2$, $21 \le k \le 25-$ скидання швидкості $j = 3$, $26 \le k \le 33-$ $j = 1$, $34 \le k \le 39-$ $j = 3$, $40 \le k \le 50- j = 2$. При описі адаптивного алгоритму оцінювання СКВ шумів збудження для різних типів руху МБПЛА встановлено: $a_1 = 1$ м/с; $a_2 = 1$м/с^2.; $a_3 =$ 7 м/с^3. РЛС і відеокамера розташовані сумісно в центрі прямокутної СК. Помилки вимірювання координат РЛС встановлено $\sigma_\beta^{\text{РЛС}} = 0.1$ град., $\sigma_\varepsilon^{\text{РЛС}} = 0{,}1$ град., $\sigma_r^{\text{РЛС}} = 20$ м, $\sigma_{\dot{r}}^{\text{РЛС}} = 10$ м/с, а помилки вимірюваннявідеокамери $\sigma_\beta^{\text{В}} = 0.1$ град., $\sigma_\varepsilon^{\text{В}} = 0{,}1$ град. Кількість реалізацій метода Монте-Карло дорівнює 100.

На рис. 1 показані математичні очікування $\hat{m}_x, \hat{m}_y, \hat{m}_z$ (точкові криві)і $\hat{\sigma}_x, \hat{\sigma}_y, \hat{\sigma}_z$ (штрихові криві)помилок оцінки координат МБПЛА, які визначені шляхом статистичного моделювання, та СКВ помилок оцінки $\sqrt{\hat{R}_x}, \sqrt{\hat{R}_y}, \sqrt{\hat{R}_z}$ (суцільні криві) положення об’єкту, які отримані з відповідних кореляційних матриць похибок оцінки за даними РЛС. На рис. 2 показані аналогічні залежності, отримані при комплексній обробці даних РЛС і відеокамери.

На рис. 3 показані ймовірностей розпізнавання p_{m1} (точкова крива) зависання, p_{m2} (штрихова крива) рівномірного руху, p_{m3} (суцільна крива)

маневру МБПЛА адаптивним алгоритмом за даними РЛС, а на рис. 3 – РЛС і відеокамери.

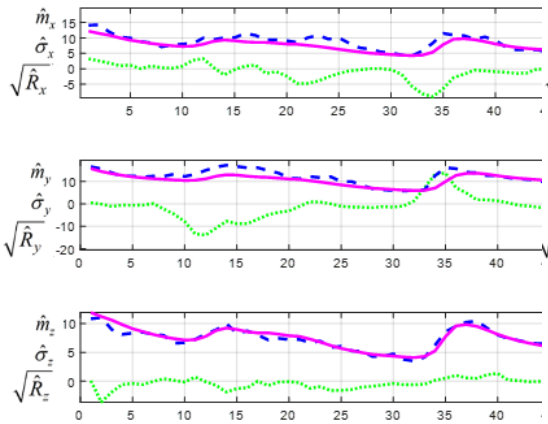


Рис. 1. Помилки оцінки координат X, Y, Z за даними РЛС

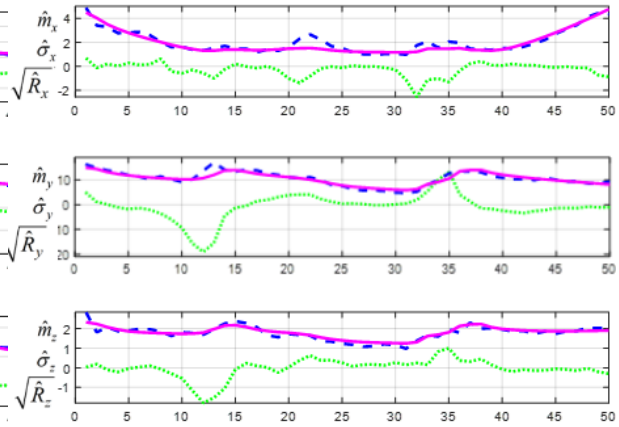


Рис. 2. Помилки оцінки координат X, Y, Z за даними РЛС і відеокамери

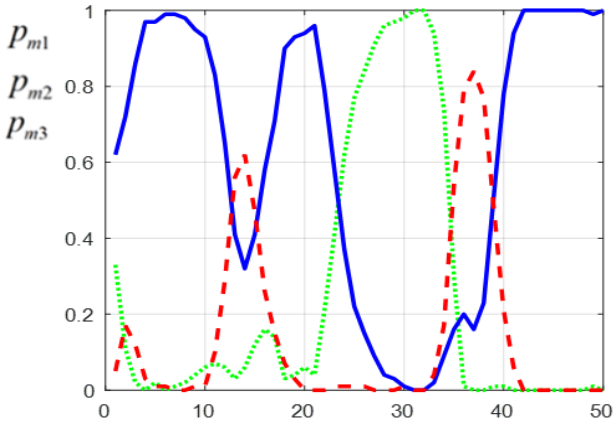


Рис. 3. Ймовірності розпізнавання видів руху МБПЛА за даними РЛС

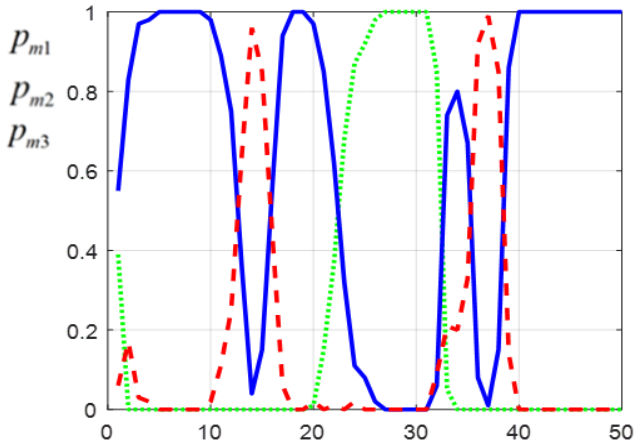


Рис. 4. Ймовірності розпізнавання видів руху МБПЛА за даними РЛС і відеокамери.

Комплексне використання даних від РЛС і відеокамери дозволило зменшити СКВ помилок визначення місцеположення МБПЛА за осями X і Zв 2-4 раз, а також підвищити ймовірність розпізнавання маневру на 18%–35%.

Література

1. Сучасний стан та проблеми протидії маловисотним, низькошвидкісним та малорозмірним БПЛА / А.С. Дудуш, В.О. Тютюнник, О.А. Резніченко, С.Ю. Гогонянц // Сучасні інформаційні технології у сфері безпеки та оборони № 1(31)/2018.
2. Жук С.Я., Товкач І.О. Методи адаптивного оцінювання параметрів руху безпілотного літального апарату на основі вимірювань сенсорної мережі. -К.: «Політехніка», КПІ ім. Ігоря Сікорського, 2019, 172 с.
3. S. Y. Zhuk, O. S. Neuimin, I. O. Tovkach and V. O. Chmelov, "Adaptive algorithm for tracking maneuvering targets in a complex jamming environment for a radar with range rate measurement," *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET),* Lviv-Slavske, Ukraine, 2020, pp. 249-254, doi: 10.1109/TCSET49122.2020.235433.

УДК 621.396.96

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ МІМО ДЛЯ ВИЯВЛЕННЯ ЦІЛЕЙ У СКЛАДНІЙ ЗАВАДОВІЙ ОБСТАНОВЦІ

Олійник М.В.
Радіотехнічний факультет КПІ ім. Ігоря Сікорського, Україна
E-mail: oliinyk.ak@gmail.com

USING MIMO TECHNOLOGY FOR TARGET DETECTION IN A COMPLEX INDUSTRIAL ENVIRONMENT

Detection of radar targets in difficult conditions thanks to the construction of a distributed radar system based on MIMO technology.

Стрімкий розвиток технологій, та їх активне впровадження призводять до швидкого покращення характеристик БПЛА. Проблема їх виявлення актуальна як у цивільному, так і у військовому секторі. Об’єкти такого типу можна охарактеризувати наступним чином [1]: мала ефективна площа розсіювання, велика швидкість руху, складна просторова конфігурація, використання радіопрозорих матеріалів, мала висота польоту. Такі цілі є дуже складними для виявлення за допомогою традиційних, моностатичних радіолокаційних систем (РЛС). У такого роду системах приймач та передавач працюють на одну антену або антенну систему, як на рис. 1а .

Пропонується інший підхід для виявлення БПЛА в складних умовах, а саме, застосовування РЛС, у яких рознесені у просторі передавач та приймач радіолокаційного сигналу. Крім того для опромінення цілі з різних ракурсів та виключення «сліпих» зон можуть застосовуватися декілька передавачів.

На відміну від моностатичних радіолокаційних системах, у бістатичних РЛС приймач та передавач рознесені, а використання декількох приймачів дозволяє отримувати відбиті під різними кутами сигнали від цілі, що збільшує ймовірність її виявлення [2], можлива конфігурація такої системи показана на рис. 1б. Як і у випадку моностатичних систем, у бістатичних існують складнощі у виявленні малорозмірних цілей, для вирішення яких потрібно покращувати енергетичні характеристики, що призводить до суттєвого підвищення складності таких систем. Також існують фізичні обмеження дальності виявлення маловисотних цілей, які вирішуються тільки збільшенням щільності радіолокаційного поля виявлення, наслідком чого є виникнення проблеми взаємного впливу різних систем одна на одну. Для вирішення такого роду проблем існують технології часового, частотного, кодового розділення. При такій організації систем спостерігається неефективне використання енергії відбитого від цілі сигналу, приймач

придушує сигнали, що передані іншими системами, оскільки вони для нього є завадою. Логічним продовження є об'єднання таких систем у одну, та взаємна обробка сигналів від усіх передавачів. Multiple Input Multiple Output (MIMO). У радарних системах, що використовують цю технологію, декілька рознесених передавачів випромінюють ортогональні сигнали, а приймачі приймають суму відбитих від цілей сигналів, приклад такої системи наведено на рис. 1в [3].

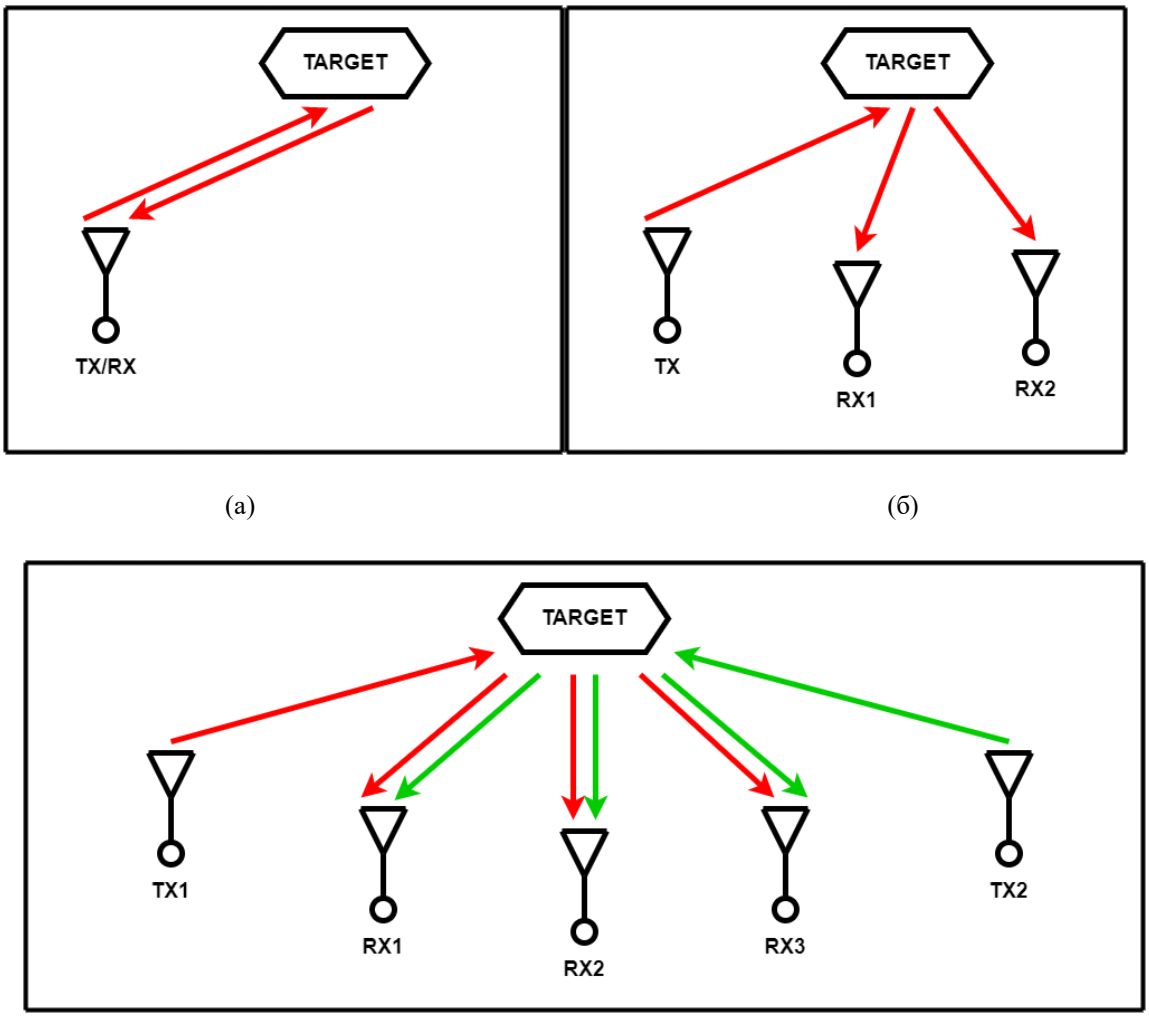


Рис.1. Радарні системи: (а) моностатичні, (б) бістатичні, (в) MIMO.

Недоліком використання цієї технології є складність обробки інформації приймачами, але просторове рознесення приймачів та передавачів призводить до зменшення ймовірності виявлення приймачів, та підвищення живучості РЛС. Передавачі можуть бути досить простими, і, відповідно, дешевими.

Для організації одночасного опромінення цілі можна використовувати кодове або частотне розділення сигналів. Часове розділення у даному випадку не підходить, оскільки з додаванням кожного передавача

зменшується частота сканування простору. Частотне розділення сигналів також не дуже ефективне у даному випадку, оскільки приймачі повинні приймати усю смугу частот, що робить їх складними та, відповідно, дорогими. Оптимальним вибором є застосування кодового розділення сигналів, а саме фазокодова маніпуляція з використанням М-послідовностей [4] .

Приймач отримує комбінацію різних відбитих сигналів від цілі, і застосовуючи методи оптимальної фільтрації, визначає сигнал що був переданий кожним з передавачів. Визначаючи азимути приходу сигналу від цілі, та знаючи точне положення приймачів, використовуючи методи пеленгації, можна визначити координати цілі. Застосування такого методу потребує тільки інформацію про азимут, а отже немає необхідності у синхронізації моменту передачі імпульсу, що спрощує конструкцію передавачів, дозволяє збільшити їх кількість та зменшити негативний вплив від їх втрати.

Приймач визначає пеленг на ціль, використовуючи сигнали від різних передавачів, що, за допомогою використання різних методів комплексування даних, дає можливість збільшити точність вимірювання азимуту, і, відповідно, точність визначення координат. Прийом сигналу опроміненої з різних напрямків цілі дозволяє підвищити якість виявлення цілі з малою еквівалентною площею розсіювання.

Висновок. Отже, застосування рознесеної у просторі радіолокаційної системи, що побудована на основі технології MIMO, дозволяє побудувати радарну систему з радіолокаційним полем високої енергетичної щільності для контролю простору зі складною конфігурацією, та забезпечити ефективне виявлення і супроводження маловисотних та малорозмірних цілей.

Література

1. C. Zhou, Y. Liu and Y. Song, “Detection and tracking of a UAV via hough transform” 2016 CIE International Conference on Radar (RADAR), Guangzhou, 2016, pp. 1-2.
2. J. Willis and D. Hugh, “Advances in Bistatic Radar”, Edited by Nicholas Griffiths, SciTech Publishing Inc., 2007, pp. 92-95.
3. J. Li, P. Stoica, MIMO radar signal processing. New Jersey: Wiley, 2009, pp. 365-368.
4. I. Pasya and T. Kobayashi, "Detection performance of M-sequence-based MIMO radar systems considering phase jitter effects," *2013 IEEE International Symposium on Phased Array Systems and Technology*, Waltham, MA, USA, 2013, pp. 394-398.

УДК 621.396.623

АНАЛІЗ ЕНЕРГЕТИЧНИХ ХАРАКТЕРИСТИК FMCW РАДАРУ МІЛІМЕТРОВОГО ДІАПАЗОНУ НА БАЗІ FPGA

Маленчик Т.В.
Радіотехнічний факультет
КПІ ім. Ігоря Сікорського, Україна
E-mail: sparrow@.ex.ua

ANALYSIS OF ENERGY CHARACTERISTICS OF THE FMCW FPGA-BASED MILLIMETER RANGE RADAR

An analysis of the influence on the energy characteristics on the detection range of UAV FMCW radar based on FPGA XC7Z020-1CLG484C was conducted.

Застосування малорозмірних безпілотних літальних апаратів (БПЛА) набуло широкого використання в різних сферах життєдіяльності. Тому актуальною є задача виявлення таких об’єктів, для запобігання згубним діям внаслідок їх несанкціонованого проникнення. Оптичні системи виявлення залежать від кількості освітлення, яке потрапляє на давач, тому можуть працювати лише в світлий період доби [1]. В свою чергу радіолокаційна система виявлення здатна працювати незалежно від кількості освітлення, часу доби, погодних умов, тощо [2].

Перспективним засобом виявлення малорозмірних БПЛА FMCW (Frequency modulated continuous wave) радар на базі FPGA (Field-Programmable Gate Array) з порівняно меншою вартістю, підвищеною надійністю та швидкодію. Такі радіолокаційні системи мають ряд переваг:

- можливість вимірювання дуже малих відстаней до цілі (мінімальна вимірювана дальність порівняна з довжиною хвилі);
- можливість одночасного виміру дальності до цілі та її радіальної швидкості [3];
- дуже висока точність виміру дальності;
- обробка сигналів здійснюється в діапазоні низьких частот, що спрощує реалізацію схем обробки;
- краща безпека через відсутність імпульсного випромінювання з великою імпульсною потужністю;
- можливість програмної реалізації алгоритмів обробки сигналів [4].

В даній роботі проведено аналіз впливу енергетичних характеристик на дальність виявлення БПЛА FMCW радаром на базі ПЛІС (XC7Z020-1CLG484C [5]).

Характеристики створеного радара наведені в табл. 1.

Таблиця 1.

Параметр	Мін. знач.	Типове	Макс. Знач.	Одиниця
АЦП частота вибірок		80		Мвиб/с
Смуга пропускання		0.5		ГГц
Частотний діапазон	33.5	34	34.1	ГГц
Період ЛЧМ		50		мкс
CW вихідна потужність		10		мВт
Коефіцієнт підсилення антен		29		дБ

Для розрахунку теоретичної максимально досяжної дальності виявлення FMCW радіолокатором використано рівняння радіолокації (1) [6] та прийнято наступні вихідні дані:

$$R_{\max} = \left[\frac{P_{\mathrm{CW}} G^2 \lambda^2 \sigma_{\mathrm{T}} L_2}{(4\pi)^3 k T_0 F B (SNR_{\min}) L_1 SRF} \right]^{\frac{1}{4}}, \qquad (1)$$

де $P_{\mathrm{CW}} = 10$дБм - середня потужність CW передавача;

$G = 29$ дБ - коефіцієнт підсилення рупорної антени; $\lambda = c / f_0 = 3\times10^8 / 34\times10^9 \approx 8{,}8$ мм - довжина хвилі;

σ_{T} - ефективна площа розсіювання (ЕПР) БПЛА;

$k = 1{,}38\times10^{-23}$ Дж/К - стала Больцмана;

$T_0 = 290$ К - абсолютна температура приймача;

$B = 500$ МГц - смуга пропускання приймача;

$L_2 = 0.9$ - коефіцієнт двостороннього атмосферної передачі;

$L_1 = 8$ дБ - коефіцієнт загальних втрат;

$SNR_{\min}$ - мінімальне значення відношення сигнал/шум (ВСШ) необхідне для виявлення;

$SRF = 1/50\times10^6 = 20$ кГц - частота повторення ЛЧМ сигналу;

$F = 1.9$ дБ - коефіцієнт шуму приймача;

На рис. 1 наведено залежність ВСШ $SNR_{\min}$ від дальності $R_{\max}$ для ЕПР $\sigma_{\mathrm{T}} = 0{,}1\text{м}^2; 0{,}01\text{м}^2$ [7]. На рис.2 приведена залежність дальності $R_{\max}$ від потужності передавача P_{cw}, при ВСШ 10 дБ.

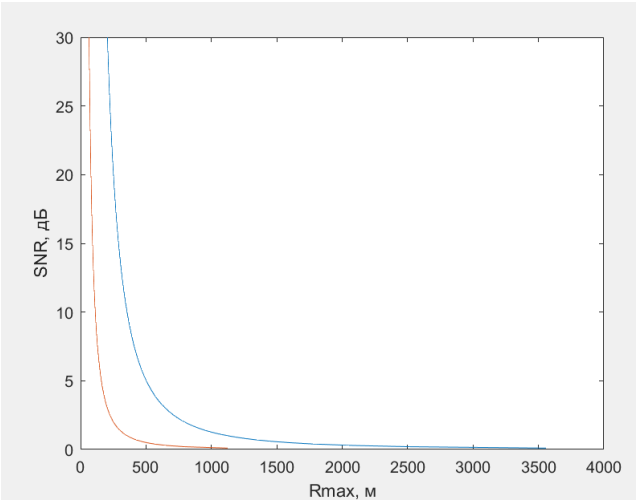


Рис. 1. Залежності ВСШ від дальності.

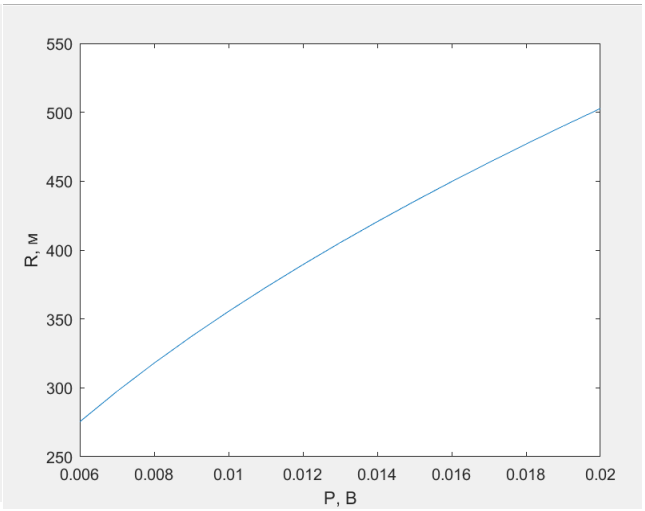


Рис. 2. Залежність дальності від потужності випромінення.

Отже, максимальна дальність виявлення БПЛА з ЕПР 0.1м^2 за допомогою FMCW радару може бути 320 – 350 м при ВСШ 10 дБ, при імовірності правильного виявлення не менше 0.8. При використанні цифрової обробки сигналу, такої як , узгодженої фільтрації та когерентне накопичення сигналу дальність виявлення може бути збільшена.

Література

1. E. Hyun, W. Oh and J. -H. Lee, "Multi-target detection algorithm for FMCW radar," 2012 IEEE Radar Conference, Atlanta, GA, USA, 2012, pp. 0338-0341, doi: 10.1109/RADAR.2012.6212161.
2. Ha, Jae Kwon, Chang Kyun Noh, Jin Seop Lee, Ho Jin Kang, Yu Min Kim, Tae Hyun Kim, Ha Neul Jung, Sang Hwan Lee, Choon Sik Cho, and Young Jin Kim. 2021. "RF Transceiver for the Multi-Mode Radar Applications" Sensors 21, no. 5: 1563. https://doi.org/10.3390/s21051563
3. N. F. M. Ariffin, F. N. M. Isa and A. F. Ismail, "FMCW Radar for Slow Moving Target Detection: Design and Performance Analysis," 2016 International Conference on Computer and Communication Engineering (ICCCE), 2016, pp. 396-399
4. Santos, D., Sebastião, P., & Souto, N. Low-cost SDR based FMCW radar for UAV localization. In 2019 22nd International Symposium on Wireless Personal Multimedia Communications (WPMC) IEEE, 2019. p. 1-6.
5. Zynq-7000 SoC Data Sheet.
6. Mohinder J., Fmcw Radar Design. Publisher: Artech House, 2018.
7. Farlik J, Kratky M, Casar J, Stary V. Multispectral Detection of Commercial Unmanned Aerial Vehicles. Sensors. 2019; 19(7):1517. https://doi.org/10.3390/s19071517

УДК 621.396.623

АВТОНОМНИЙ ДАВАЧ СЕЙСМІЧНИХ ХВИЛЬ ДЛЯ ЗАДАЧІ ОХОРОНИ ПЕРИМЕТРА

Вістизенко Є. В., Мовчанюк А.В.
Радіотехнічний факультет КПІ ім. Ігоря Сікорського, Україна
E-mail: vev18@ukr.net

AUTONOMOUS SEISMIC WAVE SENSOR FOR THE PROBLEM OF PERIMETER PROTECTION

Seismic sensors are used to detect seismic waves propagating in the ground. The publication will consider the creation of an autonomous seismic sensor to detect a person using seismic waves generated by human steps, with data processing on the edge.

Сейсмічні давачі використовуються для виявлення сейсмічних хвиль, що поширюються в ґрунті. Детектування сейсмічних хвиль застосовується для вирішення великої кількості завдань від георозвідки, промислового моніторингу до застосування в охороні периметра. В даному випадку буде розглянуто створення сейсмічного сенсора для виявлення людини за допомогою збуджених їм при ходьбі сейсмічних хвиль.

В рамках проведених авторами досліджень, була розроблена структурна схема автономного давача сейсмічного сигналу (рис.1), що має задовольнити вимоги наступні основні вимоги:

- автономність не менше ніж 1 рік;
- наявність радіо-інтерфейсу;
- дальність передачі даних до 2 км;
- можливість часової синхронізації давачів;
- встановлення давача в ґрунт без додаткового устаткування.

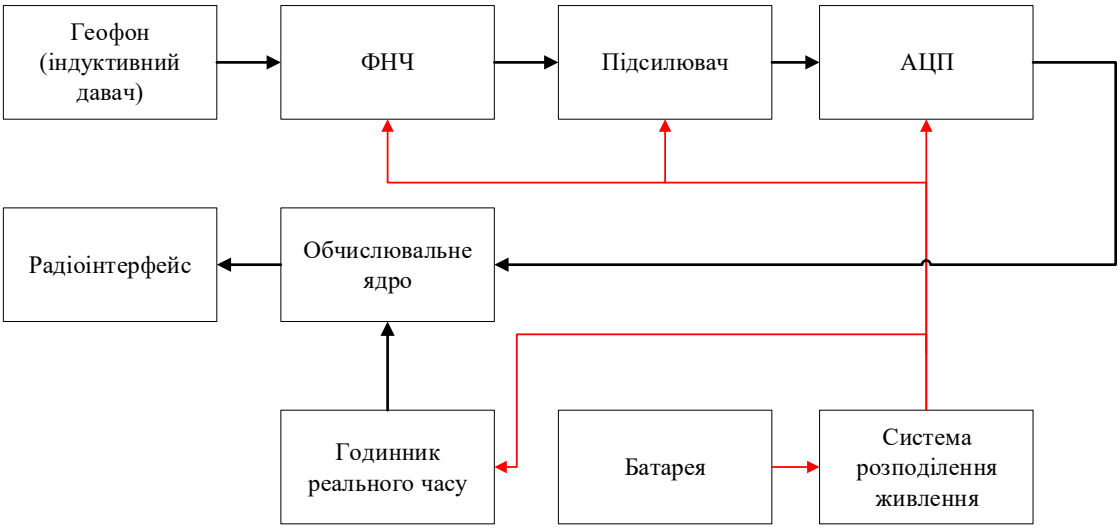


Рис.1. Структурна схему автономного сейсмічного давача.

Розглянемо структурну схему (рис.1) більш детально. Сигнал буде отримуватися з індуктивного давача сейсмічних сигналів. Частотна смуга отриманого сигналу обмежується фільтром нижніх частот до рівня 1кГц. Так як частота зрізу фільтра дуже низька, то для забезпечення максимальної «якості» сигналу буде використано активний фільтр.

Підсилювач виконаний на інструментальному операційному підсилювачі INA129 задля зменшення рівня синфазної завади та отримання можливості регулювати коефіцієнт підсилення одним елементом. До схеми підсилювача, у ланку регулювання коефіцієнту підсилення, був доданий цифровий потенціометр, задля можливості адаптації давача до місця встановлення та максимального використання динамічного діапазону АЦП. Керування коефіцієнтом підсилення виконується обчислювальним ядром в межах від 100 до 600.

Сигнал з виходу підсилювача подається на АЦП та дискретизується. Тактова частота обрана 2000 Гц для задоволення вимог по частоті Найквіста для записаного сигналу. Була використана окрема мікросхема АЦП (ADS1246) через значно більшу розрядність ніж у вбудованого АЦП обчислювального ядра (24 проти 14ти біт), що дозволяє отримати динамічний діапазон АЦП в 144 дБ.

Класифікація сигналів з сейсмічного давача виконується на обчислювальних потужностях мікроконтролера STM32L476.

В склад автономного давача була додана мікросхема годинника реального часу задля синхронізації мережі давачів та можливості додавати до сигналу спрацювання мітки часу. В якості годинника реального часу використана мікросхема DS3231, що забезпечує максимальну точність в +/-2 ppm, та споживання струму на рівні 200мкА в активному режимі та 110мкА в режимі очікування [1].

Після класифікації отриманого сигналу обчислювальним ядром, в випадку виявлення цілі, сигнал про спрацювання буде відправлений на центральну станцію по радіоканалу. Так як необхідна швидкість передачі даних не перевищує 1кБ/с, а вимоги по автономності вимагають використовувати максимально енергоефективні технології передачі даних, був обраний радіо інтерфейс LoRa [2].

До особливостей даної технології можна віднести:

- високий рівень завадозахищеності;
- велика дальність передачі даних (до 15 км);
- невеликий струм споживання;
- використання неліцензованих частотних діапазонів (433, 868, 915 МГц) .

Малопомітність передачі даних та висока завадостійкість забезпечена використанням технології розширення спектру сигналу, а саме CSS(Chirp spread spectrum). Для розширення спектру застосовується лінійна частотна модуляція, яка дозволяє збільшити дальність передачі без збільшення потужності передавача через можливість декодувати сигнал, що знаходиться нижче рівня шуму.

У нашому випадку автономний давач буде виступати кінцевим пристроєм. У якості модуля, що буде відповідати за забезпечення передачі по протоколу LoRa, був обраний LoRa-E5-HF на базі мікросхеми SX1262 компанії Semtech [3]. Керування модулем відбувається обчислювальним ядром по протоколу UART за допомогою AT-команд.

Для живлення автономного давача буде використовуватися літій-тіоніл-хлоридні батареї (Li-SOCl2), а саме 3 шт. LS33600 від компанії SAFT. Ці батареї дозволяють працювати в температурному діапазоні від -60 до +85 градусів Цельсія. Сумарна ємність трьох батарей буде складати 51000 мА/год, що при середньому розрахунковому споживанні в 5 мА (при 10% часу роботи давача в режимі обробки при виявленні сейсмічної активності), дозволить давачу пропрацювати 425 днів, що задовольняє початкові вимоги до давача.

Цікавою особливість даних батарей є стабільність вихідної напруги в процесі роботи. Згідно з графіком наведеним в документації [4], при малих струмах розряду (а в нашому випадку він буде складати 1,66 мА) напруга на батареї буде залишатися стабільною майже до повної втрати ємності. До того ж, вихідна напруга батареї складає 3,6В, що знаходиться в межах допусків на напругу живлення для всіх елементів системи. Це дозволяє не використовувати схеми стабілізації напруги живлення, що здешевлює давач і підвищує надійність. Єдиною необхідною умовою є схема балансування батарей живлення задля рівномірного розряду усіх трьох елементів живлення. В найпростішому випадку така схема буде складатися з трьох діодів, кожний з яких послідовно ввімкнений з одним з елементів живлення. Це дозволить уникнути перетікання струмів від одного елементу живлення до іншого.

Наведена структура давача та технічні рішення продемонстровані в даному матеріалі, дозволяють отримати виріб оптимізований по тактико технічним характеристикам і ціновим показникам. В подальшому даний виріб має пройти дослідну експлуатацію з отриманням відповідних висновків.

Література

1. DS3231 Datasheet [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: https://datasheets.maximintegrated.com/en/ds/DS3231.pdf.
2. LoRa опис протоколу [Електронний ресурс] – Режим доступу до ресурсу: 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.
3. LoRa-E5 Datasheet [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://files.seeedstudio.com/products/317990687/res/LoRa-E5%20module%20datasheet_V1.0.pdf.
4. LS 33600 Datasheet [Електронний ресурс]. – 2010. – Режим доступу до ресурсу: https://www.batterystation.co.uk/content/datasheets_MSDS/Saft/Saft%20LS33600 %20Product%20Data%20Sheet.pdf.

УДК 621.396.4

МОДЕЛЬ ПРИЙНЯТТЯ РІШЕННЯ ПО ТРАЄКТОРІЇ ПОЛЬОТУ ТЕЛЕКОМУНІКАЦІЙНОЮ АЕРОПЛАТФОРМОЮ ДЛЯ ЗБОРУ ДАНИХ МОНІТОРИНГУ З ВУЗЛІВ БЕЗПРОВОДОВОЇ СЕНСОРНОЇ МЕРЕЖІ

Гримуд А.Г., Романюк В.А.
Військовий інститут телекомуникацій та інформатизації, Україна
E-mail: romval2016@gmail.com

DECISION-MAKING MODEL ON THE FLIGHT TRAJECTORY OF A TELECOMMUNICATION AIRPLANE PLATFORM FOR MONITORING DATA COLLECTION FROM WIRELESS SENSOR NETWORK NODES

A situational model for constructing a trajectory for flying around UAVs over wireless sensor network nodes is proposed to achieve the specified objective functions: minimum data collection time, maximum network lifetime.

Розглядається безпроводова сенсорна мережа (БСМ) зі стаціонарними наземними вузлами, які розташовані на важкодоступній (постраждалій від надзвичайної ситуації) території в умовах відсутності будь-якої телекомунікаційної інфраструктури. БСМ характеризується наступними параметрами: значна розмірність (сотні, тисячі вузлів), обмеженість ресурсів вузлів (енергія батареї, продуктивність процесора, пам’ять, потужність передавача, тощо). Збір інформації моніторингу з вузлів БСМ в умовах відсутності зв’язності між вузлами можливий з застосуванням мобільних роботів або телекомунікаційних аероплатформ (ТА). Сенсорні вузли здійснюють моніторинг певних параметрів зовнішнього середовища (об’єктів зон свого контролю), зберігають ці дані та при появі ТА в зоні їх радіозв’язку передають дані до ТА.

Основними цільовими функціями процесу збору даних з вузлів БСМ ТА можуть бути: мінімізація часу (граничний час) збору даних $T_{зб}$, максимізація часу (визначений час) функціонування мережі $T_ф$, мінімізація кількості задіяних ТА [1, 2]. Виконання цих задач залежить від рішення по траєкторії польоту ТА. Найпростіше рішення – обліт всієї площі розташування вузлів БСМ (можливі різні маршрути обльоту – спіраллю, зигзагом, змійкою тощо), однак це рішення призводить до значного часу обльоту ТА. Другий спосіб – віртуальна кластеризація мережі, визначення в кластерах точок збору даних (зазвичай в центрі кластеру) та побудова траєкторії польоту ТА між точками збору.

Пропонується ієрархічна модель прийняття рішень по визначенню траєкторії польоту ТА для збору даних моніторингу з вузлів БСМ з реалізацією визначених цільових функцій за рівнями: вся мережа, конкретний кластер, ТА-група вузлів, ТА-окремий вузол [1, 2] (рис. 1):

1. На мережевому рівні досягнення цільових функцій відбувається визначенням кількості віртуальних кластерів та їх розмірів (шляхом

визначення висоти польоту ТА, діаграми спрямованості антени). Проводиться віртуальна однорідна кластеризація БСМ з адаптацією розмірів кластерів (використовується алгоритм кластерного аналізу FOREL) з врахуванням координат вузлів, їх взаємного розташування та пріоритету цільових функцій.

2. На рівні кластера визначається кількість та локації точок зависання ТА для збору Q_k в кожному k-му кластері з врахуванням: параметрів груп вузлів та окремих вузлів (взаємне розташування, наявна енергія вузлів, обсяг даних моніторингу $V_{дм}$), пріоритету цільових функцій шляхом додаткової неоднорідної кластеризації [1].

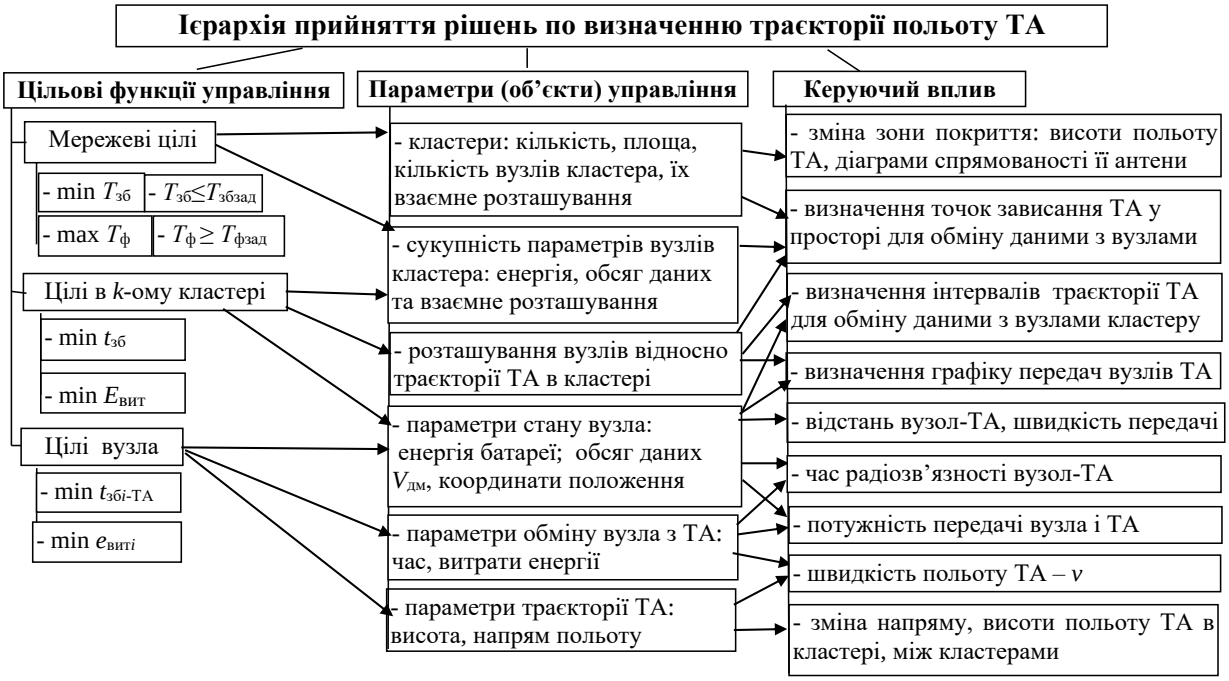


Рис. 1. Модель прийняття рішень по визначенню траєкторії польоту ТА.

3. На рівні мережі будується базовий маршрут польоту ТА з використанням алгоритму пошуку найкоротшого шляху (вирішення задачі комівояжера). Ця задача відноситься до класу NP-повних. Тому на практиці застосовують евристичні алгоритми, які надають наближене рішення, але мають незначну обчислювальну складність. Для побудови маршруту польоту в кластеризованій мережі (між точками збору даних) були проведені дослідження ефективності евристичних алгоритмів, які запропоновані дослідниками для БСМ: найближчого сусіда, за спіраллю, за квадратами, опуклої оболонки (Convex Hull Insertion Heuristic) та інші. Результати моделювання продемонстрували ефективність алгоритму опуклої оболонки для пошуку найкоротшого шляху в кластеризованій мережі, тому він визначений в якості базового.

4. В кожному кластері корегується базовий маршруту польоту ТА за рахунок методу ситуаційного управління, який використовує розроблену базу правил продукційного типу: ЯКЩО <умова>, ТОДІ <дія> [2] та реалізує відповідну схему рішень (рис. 2). Умова описується обмеженою кількістю

ситуацій (розташування кожного вузла відносно прийнятої траєкторії польоту ТА, наявний обсяг даних та енергія батарей вузлів), а дія (рис. 1) реалізує керуючі впливи, які спрямовані для досягнення цільової функції. Наприклад, зміна відстані ТА-вузол (за рахунок зміни траєкторії) дозволяє оптимізувати час обміну між ними (пропонується використовувати MAC-протокол з адаптацією швидкості передачі в залежності від співвідношення сигнал/шум) та регулювати витрати енергії вузла $e_{i\text{вит}}$. Менша відстань між вузлом та траєкторією польоту ТА дозволяє зменшити витрати енергії батареї цього вузла, збільшити швидкість передачі даних (зменшити час збору), однак призводить до збільшення довжини траєкторії. І навпаки.

Для зменшення варіантів перебору по знаходженню оптимальної траєкторії обльоту вузлів та збору даних запропоновані метаправила.

5. Відповідно до цільових функцій плануються інтервали збору даних на траєкторії ТА, визначаються додаткові точки збору даних та графік обміну вузлів з ТА в умовах їх конкуренції.

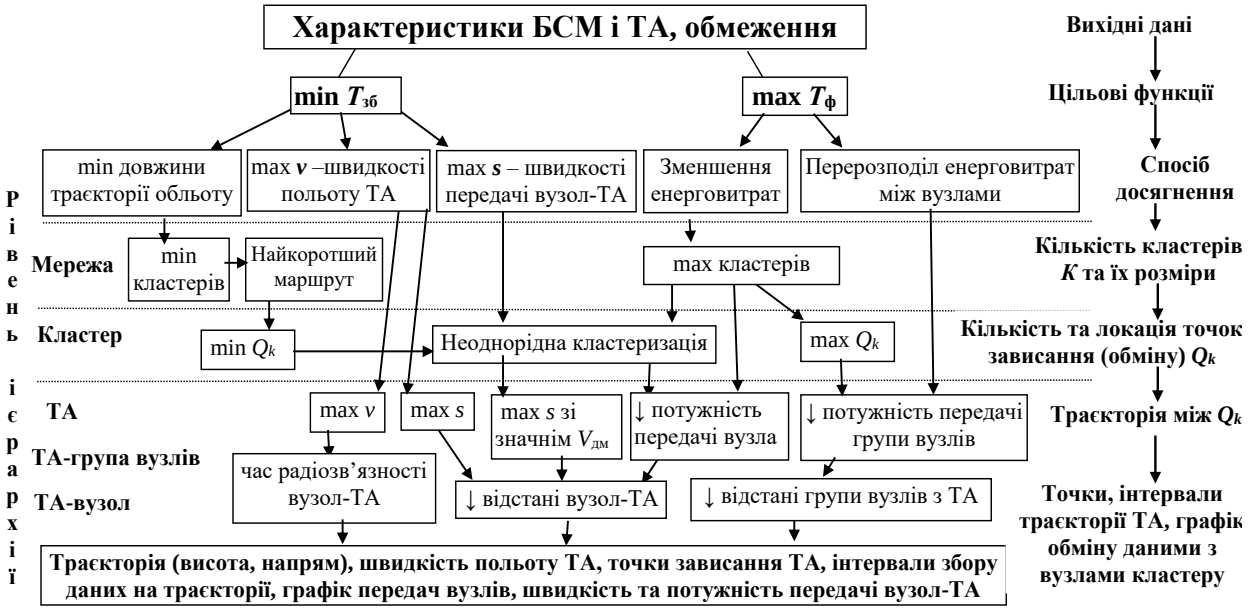


Рис. 2. Схема визначення траєкторії польоту ТА для збору даних з вузлів БСМ.

Результати імітаційного моделювання розробленої моделі показали можливість зменшити час збору даних на 10 – 15% або підвищити час функціонування мережі на 12 – 17% при задоволенні ресурсних обмежень в порівнянні з відомими рішеннями.

Література

1. Hrymud A., Romaniuk V. Modifying a method for direct data collection by a telecommunication aerial platform from nodes of wireless sensor networks. Eastern-European Journal of Enterprise Technologies, 2022, 4 (9 (118)), 15 – 29. https://doi.org/10.15587/1729-4061.2022.263559.
2. Гримуд А., Романюк В. Модель пошуку траєкторії польоту телекомунікаційною аероплатформою для збору даних з вузлів кластеризованої бездротової сенсорної мережі військового призначення. Збірник наукових праць Центру воєнно-стратегічних досліджень НУО імені Івана Черняховського № 1(74), 2022. С. 118 – 128. https://doi.org/10.33099/2304-2745/2022-1-74/118-128.

УДК 621.3

INVESTIGATION OF THE PHENOMENON OF RADIO RECEPTION BLOCKING OF UNPILOTED AERIAL VEHICLES

Blahaia O.S.
Faculty of Air Navigation,
Electronics and Telecommunications,
National Aviation University, Ukraine
E-mail: blolexandra@gmail.com

ДОСЛІДЖЕННЯ ЯВИЩА БЛОКУВАННЯ РАДІОПРИЙМАЛЬНОГО ПРИСТРОЮ БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТА

Проведено дослідження на тему явище блокування радіоприймального пристрою БПЛА, маючи на меті дослідити явище блокування радіоприймального пристрою БПЛА навмисною радіозавадою для позбавлення його управління. Робота присвячена явищу блокування, оскільки воно найбільш доступне і найбільш легке в прогнозуванні та в аналізі для можливого застосування.

A study has been carried out on the phenomenon of blocking the UAV radio receiver, with the aim of investigating the phenomenon of blocking the UAV radio receiver by intentional radio interference to deprive it of control. The work is devoted to the phenomenon of blocking, since it is the most accessible and the easiest to predict and analyze for possible applications.

The relevance of the work is that among the possible technical ways of damaging the quality of functioning of the equipment of unmanned aerial vehicles are very effective, but very complex and highly valuable.

Therefore, such a method is relevant today, excluding the possibility of the operation of UAV equipment, which would be quite effective, but at the same time simple to implement.

The following tasks were set and completed:

1) Carry out a literary review of UAVs, their equipment and a description of the phenomenon of blocking the radio receiver;

2) Analyze the known methods of deprivation of control and propose a method that would be effective, but not expensive;

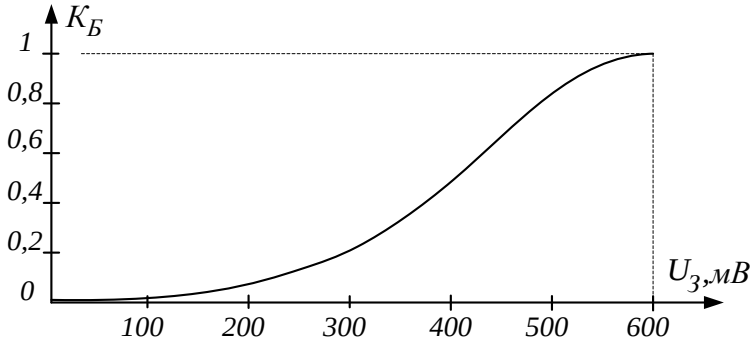
3) Perform a physical simulation of the blocking phenomenon to identify its threshold.

The object of the study was the phenomenon of signal blocking in a radio receiver.

The subject of research is a method of blocking the UAV communication channel, which can be used in fleeting changes in environmental conditions.

In the course of the study, a theoretical and experimental study of the phenomenon of blocking a radio station in the meter range was carried out, which consists in reducing the gain of the input stage under the influence of interference. This is what will deprive the UAV of a control signal. Therefore, I carried out theoretical calculations and an experimental study of the dependence of the blocking coefficient on the level of interference.

The blocking of the input stage of the receiver occurs due to the movement of the operating point of the current-voltage characteristic in the direction of decreasing its steepness, as shown in the graph. After conducting research, we removed the dependence of the blocking coefficient on the level of interference. The graph is shown on the slide. Behind it, I determined that at an interference level of 600 millivolts and a useful signal of 50 microvolts, complete blocking of the receiver occurred, and at the level of 450 millivolts, the blocking factor reaches 0.7 with the maximum possible 1 according to the graph, which means it is almost impossible to process the received signal.



$$K_{бл} = \frac{U_{с\,вих} - U_{\Sigma вих}}{U_{с\,вих}}$$

Conclusion. It is proposed to use the phenomenon of blocking the radio receiver by interference as an inexpensive and fairly effective way to deprive the UAS of the ability to control. An experimental study of the phenomenon of blocking a radio receiver of the meter range of radio waves by radio interference was carried out, as a result of which acceptable values of its amplitude were obtained for the complete blocking of channels for receiving control signals of unmanned aerial systems.

References

1. Unmanned aviation complexes: monogr. / V.G. Bashynskyi, V.B. Bzot, E.I. Zhilin et al. – Zaporizhzhia, 2016. – 211 p.
2. Ivanov V.O., Gabrusenko E.I., Ilnytskyi L.Ya., Shcherbina O.A. Electromagnetic compatibility of radio-electronic equipment. Tutorial. - K.: NAU, 2014. - 312 p.
3. A.G. Taranenko, Ye.I. Gabrusenko, A.G. Holubnychyi, O.A. Lavrynenko. Operational reliability management of the reserved electronic system/ Electronics and control systems No. 1(63), 2020, pp. 86-92.

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

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ НДІ ТЕЛЕКОМУНІКАЦІЙ

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

Конференцію присвячено:

125-річчю Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

20-річчю Навчально-наукового інституту телекомунікаційних систем

30-річчю кафедри Телекомунікацій

19 квітня 2023 року

Тези конференції

м. Київ

ПРОГРАМНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ ПРІТС-2022

Співголови конференції:

ІЛЬЧЕНКО М.Ю. – науковий керівник НН 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 НН інституту телекомунікаційних систем КПІ ім. Ігоря Сікорського;

КОНОНОВА І.В – к.т.н., доц., НН інституту телекомунікаційних систем КПІ ім. Ігоря Сікорського;;

ЛІСОВСЬКИЙ К.С.–в.о. голови студентської ради НН ІТС 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., доц., 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:

Авдєєнко Г.Л., к.т.н., 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., к.т.н., ст. викладач, КПІ ім. Ігоря Сікорського, ІТС, Київ;
Кравчук І.М., к.т.н., ст. викладач, КПІ ім. Ігоря Сікорського, ІТС, Київ;
Штогрина О.С., к.т.н., КПІ ім. Ігоря Сікорського, ІТС, Київ.

ТЕНДЕНЦІЇ РОЗВИТКУ РАДІОРЕЛЕЙНИХ СИСТЕМ

Кравченко І.М.
Науковий керівник: **Наритник Т.М.**
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: il.kravchenko115@gmail.com

Досліджено тенденції розвитку радіорелейних систем. Розглянуто революційну радіостанцію "точка-точка" AirFiber від компанії Ubiquiti. Розробка особливого внутрішньо-фірмового протоколу AirMax, за допомогою якого ведеться бездротова передача даних. Перехід радіорелейних систем на більш високі частоти. Перехід до автоматизації та дистанційного керування в радіорелейних системах.

TRENDS IN THE DEVELOPMENT OF RADIO RELAY SYSTEMS

Kravchenko I.M.
Scientific adviser: **Narytnyk T.M.**
Educational and Scientific Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: il.kravchenko115@gmail.com

The trends in the development of radio relay systems are studied. The revolutionary point-to-point radio station AirFiber from Ubiquiti is considered. The development of a special intra-company protocol AirMax, which is used for wireless data transmission. Migration of radio relay systems to higher frequencies. Transition to automation and remote control in radio relay systems.

ІСТОРІЯ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ 4G-6 G ЗВ'ЯЗКУ У СВІТІ

Кисіль А. В.
Науковий керівник: **Наритник Т.М.**
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: linka.kisel2002@gmail.com

Більшості сучасних гаджетів потрібен інтернет і підключаються вони до нього бездротовим способом, за допомогою радіохвиль. Сукупність параметрів цих радіохвиль, технологія передачі і протоколи, за якими дані шифруються в звук, відео або текст - називається стандартом мобільного зв'язку.

A BRIEF OVERVIEW OF THE HISTORY OF THE INTRODUCTION OF 4G, 5G, 6G COMMUNICATION TECHNOLOGIES IN THE WORLD IS GIVEN

Kysil A. V.
Scientific adviser: **Narytnyk T.M.**
Educational and Scientific Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: linka.kisel2002@gmail.com

Most modern gadgets need the Internet and connect to it wirelessly, using radio waves. The set of parameters of these radio waves, the transmission technology and the protocols by which the data is encrypted into sound, video or text is called the mobile communication standard.

СТАН ТА ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ТЕРАГЕРЦОВОГО ДІАПАЗОНУ В СУПУТНИКОВОМУ ЗВ'ЯЗКУ

Луговець О.В.
Науковий керівник: **Наритник Т.М.**
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: olov20232642@gmai.com

Робота присвячена вивченню стану та перспектив використання терагерцового діапазону в супутниковому зв'язку. У статті розглядаються технічні особливості терагерцового діапазону, а також аналізуються переваги та недоліки цього діапазону в порівнянні з іншими діапазонами радіохвиль.

STATUS AND PROSPECTS OF USING THE TERAHERTZ BAND IN SATELLITE COMMUNICATION

Luhovets O.V.
Scientific adviser: **Narytnyk T.M.**
Educational and Scientific Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: olov20232642@gmai.com

This paper is devoted to the study of the state and prospects of using the terahertz band in satellite communications. The paper discusses the technical features of the terahertz band, as well as analyzes the advantages and disadvantages of this band in comparison with other radio wave bands.

ПРАКТИЧНЕ ВИКОРИСТАННЯ NETWORK DEVOPS ДЛЯ АВТОМАТИЗАЦІЇ УПРАВЛІННЯ В ІНФОКОМУНІКАЦІЯХ

Персіков М.А., Лемешко В.О., Мамон Р.В.
Науковий керівник: **Єременко О.С.**
Харківський національний університет радіоелектроніки, Україна
E-mail: mykhailo.persikov@nure.ua, valentyn.lemeshko@nure.ua, roman.mamon@nure.ua

Досліджено підходи та засоби Network DevOps, необхідні для інтеграції IT-операцій та надійного надання мережних послуг, пов’язаних із розгортанням, конфігуруванням та обслуговуванням мережної інфраструктури безпроводових телекомунікаційних мереж. Доведено, що сучасні платформи автоматизації ефективно відстежують мережні ресурси під час ініціалізації та взмозі оцінити можливості мережі щодо реалізації відповідних запитів конфігурації. Розроблено та апробовано програму мовою Python для пошуку номерів базових станцій, розташованих на колі заданного радіусу, та відстаней до них, у мережах мобільного зв’язку, яка довела свою працездатність і може використовуватись на практиці.

PRACTICAL USE OF NETWORK DEVOPS FOR MANAGEMENT AUTOMATION IN INFOCOMMUNICATIONS

Persikov M.A., Lemeshko V.O., Mamon R.V.
Scientific adviser: **Yeremenko O.S.**
Kharkiv National University of Radio Electronics, Ukraine
E-mail: mykhailo.persikov@nure.ua, valentyn.lemeshko@nure.ua, roman.mamon@nure.ua

Explored Network DevOps approaches and tools needed to integrate IT operations and reliably deliver network services related to the deployment, configuration, and maintenance of wireless telecommunications network infrastructure. It has been proven that modern automation platforms effectively monitor network resources during initialization and can assess the network's capabilities to implement relevant configuration requests. A Python program has been developed and tested for finding the number of base stations located on a circle of a given radius and the distances to them in mobile communication networks. It has proven its efficiency and can be used in practice.

АНАЛІЗ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ СТЕГАНОГРАФІЧНОГО ПЕРЕТВОРЕННЯ

Майба М.А.
Науковий керівник: **Єременко О.С.**
Харківський національний університет радіоелектроніки, Україна
E-mail: mykola.maiba@nure.ua

Досліджено найбільш популярні засоби стеганографічного захисту даних. Проаналізовано модуль StegCloak, призначений для приховування таємної інформації в середині тексту шляхом стиснення та шифрування секрету перед його маскуванням. Значною перевагою використання StegCloak для вирішення задачі забезпечення захисту інформації є те, що повідомлення буде зашифровано всередині звичайного тексту. Такий підхід гарантує додатковий захист, тому що під час використання даного алгоритму стеганографічного перетворення користувач не буде привертати до себе зайвої уваги. Також з переваг можливо зазначити те, що StegCloak не тільки приховує секрет, але й захищає його паролем на вибір користувача.

ANALYSIS OF INFORMATION PROTECTION MEANS WITH STEGANOGRAPHIC TRANSFORMATION

Maiba M.A.
Scientific adviser: **Yeremenko O.S.**
Kharkiv National University of Radio Electronics, Ukraine
E-mail: mykola.maiba@nure.ua

The most popular means of steganographic data protection were studied. We analyzed the StegCloak module, designed to hide secret information inside the text by compressing and encrypting the secret before masking it. A significant advantage of using StegCloak to solve the problem of securing data is that the message will be encrypted inside plain text. Such an approach guarantees additional protection because the user will not draw unnecessary attention to himself when using this steganographic transformation algorithm. Another advantage is that StegCloak not only hides the secret but also protects it with a password of the user's choice.

АНАЛІЗ І ДОСЛІДЖЕННЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ МЕРЕЖНОЇ БЕЗПЕКИ З УРАХУВАННЯМ БАЛАНСУВАННЯ НАВАНТАЖЕННЯ

Негре Де Бофарулл Фернандо Рафаель, Юджесой Асіл Йігіт
Науковий керівник: **Єременко О.С.**
Харківський національний університет радіоелектроніки, Україна
E-mail: fernando.rafael.negre.de.bofarull@nure.ua, asil.iihit.iudzhesoi@nure.ua

Проведено аналіз існуючих методів комплексного забезпечення мережної безпеки та якості обслуговування засобами маршрутизації шляхом реалізації балансування навантаження в сучасних мережах. Розглянуто декілька варіантів реалізації багатошляхової безпечної маршрутизації з балансуванням і без балансування навантаження. Водночас розрахунок безпечного мультишляху проводився з урахуванням комбінованої метрики на основі вразливостей і пропускної здатності каналів зв’язку, що входили до складу маршруту. Поставлені технологічні задачі представлено в оптимізаційній формі та проведено аналіз отриманих результатів, що довели адекватність і працездатність комплексної моделі безпечної QoS-маршрутизації.

ANALYSIS AND RESEARCH OF ENSURING NETWORK SECURITY METHODS UNDER LOAD BALANCING

Fernando Rafael Negre De Bofarull, Asil Yigit Yucesoy
Scientific adviser: **Yeremenko O.S.**
Kharkiv National University of Radio Electronics, Ukraine
E-mail: fernando.rafael.negre.de.bofarull@nure.ua, asil.iihit.iudzhesoi@nure.ua

An analysis of the existing methods of comprehensive provision of network security and Quality of Service utilizing routing through the implementation of load balancing in modern networks was carried out. Several options for implementing secure multipath routing with and without load balancing are considered. At the same time, the secure multipath was calculated, taking into account the combined metric based on the vulnerabilities and bandwidth of the communication links that were part of the route. The set technological tasks are presented in an optimization form, and the results obtained are analyzed and prove the adequacy and efficiency of the complex model of secure QoS routing.

ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ТА БЕЗПЕКИ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Юджесой Асіл Йігіт, Негре Де Бофарулл Фернандо Рафаель
Науковий керівник: **Єременко О.С.**
Харківський національний університет радіоелектроніки, Україна
E-mail: asil.iihit.iudzhesoi@nure.ua, fernando.rafael.negre.de.bofarull@nure.ua

Проведено аналіз методів, засобів і технологій відповідно до забезпечення стійкості та безпеки критичної інформаційної інфраструктури. Визначено основні вимоги безпеки, що висуваються до телекомунікаційних мереж як об'єктів критичних інформаційних інфраструктур. Відзначено, що для сталого функціонування таких об'єктів необхідна розробка комплексних рішень з урахуванням технологій безпеки, надійності, резервування та живучості. Обрано математичну модель відмовостійкої та безпечної маршрутизації фрагментованих конфіденційних повідомлень з використанням композитних шляхів у мережах критичних інформаційних інфраструктур. Проаналізовано результати моделювання обраної моделі та обґрунтовано її використання.

PROVIDING THE RESILIENCE AND SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE

Asil Yigit Yucesoy, Fernando Rafael Negre De Bofarull
Scientific adviser: **Yeremenko O.S.**
Kharkiv National University of Radio Electronics, Ukraine
E-mail: asil.iihit.iudzhesoi@nure.ua, fernando.rafael.negre.de.bofarull@nure.ua

An analysis of methods, tools, and technologies was carried out to ensure the resilience and security of Critical Information Infrastructure. The main security requirements for telecommunication networks as objects of Critical Information Infrastructures are defined. It was noted that for the sustainable functioning of such objects, it is necessary to develop complex solutions considering security, reliability, redundancy, and survivability technologies. A mathematical model of fault-tolerant and secure routing of fragmented confidential messages using composite paths in networks of Critical Information Infrastructures is chosen. The simulation results of the selected model were analyzed, and its use was justified.

ПЕРЕВАГИ ВИКОРИСТАННЯ SIEM СИСТЕМИ WAZUH ДЛЯ ПІДВИЩЕННЯ СТІЙКОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Капуста Р.Д., Горяінова К.О.
Науковий керівник: **Єременко О.С.**
Харківський національний університет радіоелектроніки, Україна
E-mail: roman.kapusta@nure.ua, karyna.horiainova@nure.ua

Проведено порівняльний аналіз низки існуючих SIEM систем з відкритим кодом та виділено переваги кожної з них. Для подальшого дослідження обрано систему WAZUH, яка містить необхідний інструментарій щодо забезпечення моніторингу та реагування на інциденти у режимі реального часу. Зазначено, що WAZUH може підтримувати необмежену кількість агентів, надаючи можливість проводити контроль та аудит операційних систем кінцевих користувачів підприємства. Обмеження щодо розгортання даної SIEM полягає у фізичній потужності обладнання, на якому буде розгорнуто сервер менеджер. Отримані результати досліджень рекомендовано для використання під час проєктування стійких і надійних систем захисту інформації підприємств.

ADVANTAGES OF USING THE WAZUH SIEM SYSTEM TO INCREASE THE RESILIENCE OF ENTERPRISE INFORMATION SECURITY

Roman Kapusta, Karyna Horiainova
Scientific adviser: **Yeremenko O.S.**
Kharkiv National University of Radio Electronics, Ukraine
E-mail: roman.kapusta@nure.ua, karyna.horiainova@nure.ua

A comparative analysis of several existing open-source SIEM systems was conducted, and the advantages of each system were highlighted. The WAZUH system was chosen for further research, which contains the necessary tools for monitoring and responding to incidents in real-time. It is noted that WAZUH can support an unlimited number of agents, providing the ability to monitor and audit the operating systems of enterprise end users. The limitation regarding the deployment of this SIEM lies in the equipment's physical capacity on which the server manager will be deployed. The obtained research results are recommended for use when designing resilient and sustainable information protection systems for enterprises.

ДОСЛІДЖЕННЯ АТАКИ "MAN-ON-THE-SIDE" ШЛЯХОМ МОДЕЛЮВАННЯ ЗАСОБАМИ WIRESHARK

Кашаіджа Джоель, Юджесой Асіл Йігіт,
Негре Де Бофарулл Фернандо Рафаель
Науковий керівник: **Єременко О.С.**
Харківський національний університет радіоелектроніки, Україна
E-mail: kashaija.joel@nure.ua, asil.iihit.iudzhesoi@nure.ua,
fernando.rafael.negre.de.bofarull@nure.ua

Проведено дослідження активної атаки "Man-on-the-Side" (MotS), у разі застосування якої кіберзлочинці можуть підслуховувати та вставляти повідомлення під час коммунікації двох сторін. Відповідаючи на запит жертви, зловмисник використовує перевагу в часі, щоб переконатися, що його повідомлення потрапить туди першим і до відповідної відповіді. Одним з методів виявлення MotS є перевірка затримки. Отже, досліджено ефективність атаки MotS з використанням Wireshark для аналізу пакетів на основі симуляції підробки ARP. Здійснено атаку Man-on-the-Side на основі таблиці спуфінгу ARP з імітацією реального середовища. Доведено, що у разі проведення атаки типу MotS можливе швидке отримання паролів від незахищеного входу.

INVESTIGATION OF "MAN-ON-THE-SIDE" ATTACK BY WIRESHARK SIMULATION

Joel Kashaija, Asil Yigit Yucesoy, Fernando Rafael Negre De Bofarull
Scientific adviser: **Yeremenko O.S.**
Kharkiv National University of Radio Electronics, Ukraine
E-mail: kashaija.joel@nure.ua, asil.iihit.iudzhesoi@nure.ua,
fernando.rafael.negre.de.bofarull@nure.ua

An active "Man-on-the-Side" (MotS) attack has been investigated, in which cybercriminals can eavesdrop and insert messages during communication between two parties. When responding to a victim's request, the attacker uses a time advantage to ensure his message arrives before the appropriate response. One method of detecting MotS is to check latency. Therefore, the effectiveness of the MotS attack was investigated using Wireshark to analyze packets based on ARP spoofing simulation. A "Man-on-the-Side" attack based on the ARP spoofing table was performed, simulating a real environment. It has been proven that in the case of a MotS-type attack, it is possible to obtain passwords from an unprotected login quickly.

СТРАТЕГІЇ ВІДМОВОСТІЙКОСТІ АРХІТЕКТУР EXTENDED CLOUD НА ОСНОВІ ПОЛІТИК

Недоступ Д.М., Солом'яний М.В.
Науковий керівник: **Єременко О.С.**
Харківський національний університет радіоелектроніки, Україна
E-mail: daniil.nedostup@nure.ua, maksym.solomianyi@nure.ua

Проведено аналіз сучасних підходів забезпечення відмовостійкості архітектур на базі Extended Cloud. В процесі використання Extended Cloud слід дотримуватися багаторівневої стратегії D^2R^2+DR (Defend, Detect, Remediate, Recover, Diagnose, and Refine). Виділено основну особливість даної стратегії, яка полягає в циклічності процесів виявлення збоїв під час функціонування мережі та їх негативні наслідки в реальному часі. Управління поведінкою телекомунікаційної системи (ТКС) виконується за рахунок використання політик для налаштування схем відмовостійкості. Таким чином, формування стратегій адаптації ТКС у реальному часі до зовнішних і внутрішних несприятливих чинників дозволяє підвищити рівень відмовостійкості.

POLICY-BASED RESILIENCE STRATEGIES FOR EXTENDED CLOUD ARCHITECTURES

Nedostup D.M., Solomianyi M.V.
Scientific adviser: **Yeremenko O.S.**
Kharkiv National University of Radio Electronics, Ukraine
E-mail: daniil.nedostup@nure.ua, maksym.solomianyi@nure.ua

An analysis of the modern approaches to ensuring the resilience of Extended Cloud-based architectures was carried out. In using Extended Cloud, a multi-level strategy of D^2R^2+DR (Defend, Detect, Remediate, Recover, Diagnose, and Refine) should be followed. The main feature of this strategy is highlighted, which consists of the cyclical nature of the detecting failures processes during the network operation and their negative impact in real-time. Management of the behavior of the telecommunication system (TCS) is performed by using policies to configure fault-tolerance schemes. Thus, developing strategies for real-time adapting TCS to external and internal adverse factors increases resilience level.

ВИМОГИ ДО ЕНЕРГЕТИЧНИХ ПАРАМЕТРІВ ІМІТАЦІЙНОЇ ЗАВАДИ КАНАЛУ УПРАВЛІННЯ ДРОНОМ

Тичинський - Мартинюк В.Ю.
Науковий керівник: **Якорнов Є.А.**
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: kyiv12@bigmir.net

Ефекту порушення управління дроном можна досягнути, якщо імітаційний сигнал буде мати достатню потужність для того, аби порушити синхронізацію в каналі управління дроном. Такого можна досягти шляхом прийому і ретрансляції сигналу управління з додаванням певних змін у параметри сигналу. Для визначення параметрів достатньої потужності сигналу імітаційної завади і вимог до енергоживлення проведені розрахунки втрат потужності сигналу управління дроном на різних етапах його руху.

Для визначення втрат на розповсюдження сигналу управління дроном застосовано набір формул Окумура – Хати для різних параметрів руху дрона у діапазоні 900 МГц. Розрахунки показали, що потужність сигналу імітаційної завади знаходиться у межах можливостей доступних на комерційному ринку радіомодулів у цьому діапазоні частот при обмежених витратах на енергоживлення та за умови забезпечення просторової розв’язки приймальної і передавальної антен радіомодуля.

REQUIREMENTS FOR ENERGY PARAMETERS OF THE SPOOFING INTERFERENCE TO THE DRONE CONTROL CHANNEL

Tychynskyi - Martyniuk V.Yu.
Scientific consultant: **Yakornov E.A.**
Educational and Scientific Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: kyiv12@bigmir.net

The drone control disruption effect can be achieved if the simulated signal has sufficient power to disrupt the synchronization in the drone control channel. This can be achieved by receiving and retransmitting the control signal with the addition of certain changes to the signal parameters. To determine the parameters of the sufficient power of the simulated interference signal and the power supply requirements, calculations were made for power losses of the drone control signal at various stages of drone movement.

To determine the propagation loss of the drone control signal, a set of Okumura-Hata formulas was applied for various parameters of the drone movement in the 900 MHz range. Calculations showed that the power of the simulated interference signal is within the capabilities of radio modules available on the commercial market in this frequency range with limited power supply costs and provided that the radio module's receiving and transmitting antennas are spatially separated.

ДОСЛІДЖЕННЯ ПОШИРЕННЯ РАДІОХВИЛЬ ДЛЯ ЗАСОБІВ ЗВ'ЯЗКУ ТА КЕРУВАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Філімончук В.М.
Науковий керівник: **Габрусенко Є.І.**
Національний Авіаційний Університет, Факультет Аеронавігації, Електроніки та Телекомунікацій, Україна
E-mail: filimonchukvaleria@gmail.com

Досліджено поширення радіохвиль в реальних умовах для тропосферної і земної хвиль в залежності від напряму, стану середовища, відстані та потужності випромінювача для вирішення задач перехоплення бпла. Знайдено найбільш раціональні способи розрахунку поширення радіохвиль: формула ідеальної радіопередачі домножена на множник розсіювання для стандартної тропосфери для тропосферних хвиль та формула Шулейкіна-Ван дер Поля для земних радіохвиль.

EXPLORATION OF EMISSION OF RADIO WAVES FOR MEANS OF COMMUNICATION AND CONTROL OF UNMANNED AERIAL VEHICLES

Filimonchuk V.M.
Scientific adviser: **Gabrusenko E.I.**
National Aviation University, Faculty of Air Navigation, Electronics and Telecommunications, Ukraine
E-mail: filimonchukvaleria@gmail.com

The emission of radio waves in real conditions for tropospheric and terrestrial waves depending on direction, environment, distance and emitter power was explored to find ways to block UAV. The most convenient ways of calculating the emission of radio waves were found: formula of perfect radio emission supplemented it with a multiplier of radio waves scattering in a standard troposphere for tropospheric radio waves and Schulekyn Van-der-Pol's methodic for radio waves.

ДОСЛІДЖЕННЯ ЯВИЩА БЛОКУВАННЯ РАДІОПРИЙМАЛЬНОГО ПРИСТРОЮ БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТА

Благая О.С.
Науковий керівник: **Габрусенко Є.І.**
Факультет Аеронавігації, Електроніки та Телекомунікацій,
Національний Авіаційний Університет, Україна
E-mail: blolexandra@gmail.com

В роботі проаналізовано залежність явища блокування від амплітуди завади, та наведено його кількісну оцінку – коефіцієнт блокування. Запропоновано поняття порогу блокування як такої величини амплітуди завади, при якій якість функціонування радіоприймального пристрою є незадовільною. Проведено експериментальне дослідження явища блокування радіоприймача метрового діапазону радіохвиль радіозавадою, в результаті якого отримані прийнятні значення її амплітуди для повного блокування каналів прийому сигналів управління безпілотних авіаційних систем.

INVESTIGATION OF THE PHENOMENON OF RADIO RECEPTION BLOCKING OF UNPILOTED AERIAL VEHICLES

Blahaia O.S.
Scientific adviser: **Gabrusenko E.I.**
Faculty of Air Navigation, Electronics and Telecommunications,
National Aviation University, Ukraine
E-mail:blolexandra@gmail.com

The dependence of the blocking phenomenon on the interference amplitude is analyzed, and its quantitative assessment is given - the blocking coefficient. The concept of the blocking threshold as such is the magnitude of the interference amplitude, at which the quality of the functioning of the radio receiver is unsatisfactory. An experimental study of the phenomenon of blocking a radio receiver of the meter range of radio waves by radio interference was carried out, as a result of which acceptable values of its amplitude were obtained for the complete blocking of receiving signal channels.

ПРОБЛЕМИ УПРАВЛІННЯ БЕЗПРОВОДОВИМИ СЕНСОРНИМИ МЕРЕЖАМИ

Орел М.В.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інституттелекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: kolaorel556@gmail.com

Сенсорні мережі є важливою складовою сучасних мереж Інтернету Речей, застосовуються в сферах контролю, безпеки, охорони здоров'я, транспорту, промисловості, розумного будинку, тощо. В роботі досліджено особливості роботи безпроводових сенсорних мереж. Виявлено основні проблеми управління безпроводовими сенсорними мережами. На основі проведеного аналізу запропоновано рекомендації щодо вдосконалення процесу управління.

PROBLEMS OF MANAGING WIRELESS SENSOR NETWORKS

Orel M.V.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: kolaorel556@gmail.com

Sensor networks are an important component of modern Internet of Things networks, used in the areas of control, security, healthcare, transportation, industry, smart home, etc. The paper investigates the features of wireless sensor networks. The main problems of managing wireless sensor networks are identified. Based on the analysis, recommendations for improving the management process are proposed.

ПУБЛІЧНИЙ ХМАРНИЙ СЕРВІС

Кугут А.С.
Науковий керівник: **Міночкін Д.А.**
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail:anot4578@gmail.com

Загальнодоступна хмара - це стороння керована платформа, яка використовує стандартну модель хмарних обчислень, щоб зробити ресурси та послуги доступними для віддалених користувачів у всьому світі. В роботі розглядаються питання архітектури, принципів та переваг роботи загальнодоступних хмарних ресурсів.

PUBLIC CLOUD SERVICE

Kugut A.S.
Scientific adviser: **Minochkin D.A.**
Educational and Scientific Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail:anot4578@gmail.com

A public cloud is a third-party managed platform that uses a standard cloud computing model to make resources and services available to remote users around the world. The work examines issues of architecture, principles and advantages of publicly available cloud resources.

АНАЛІЗ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ QOS В МУЛЬТИСЕРВІСНИХ МЕРЕЖАХ ДОСТУПУ

Глоба А. А.
Науковий керівник: **Носков В. І.**
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: marsalhejli@gmail.com

Досліджено основні методи забезпечення QoS в мультисервісних мережах доступу та розглянуто механізми забезпечення якості обслуговування.

ANALYSIS OF METHODS OF PROVIDING OF QOS IS IN THE MULTISERVICE NETWORKS OF ACCESS

Hloba A. A.
Scientific adviser: **Noskov V. I.**
Educational and Scientific Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: marsalhejli@gmail.com

The main methods of providing QoS in multi-service access networks were studied and the mechanisms of ensuring the quality of service were considered.

МОДИФІКОВАНА СИСТЕМА ЗАХИСТУ МЕРЕЖІ ІНТЕРНЕТ РЕЧЕЙ

Бушинський Д.А.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий Інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: dbushynskyi2002@gmail.com

З вдосконаленням пристроїв, збільшенням обчислювальної потужності та зменшенням споживання енергії тенденція впровадження IoT продовжиться. Однією з найскладніших тем у такому взаємопов'язаному світі мініатюрних систем і датчиків є аспекти безпеки та конфіденційності: без упевненості, що гарантується безпека приватної інформації та належний захист, користувачі не за хочуть прийняти цю нову технологію, яка непомітно інтегрується в життя. Щоб широко запровадити IoT, цю проблему слід вирішити, щоб забезпечити впевненість користувачів щодо конфіденційності та контролю особистої інформації.

До особливостей даної роботи можна віднести дослідження вирішення проблеми захисту та конфіденційності шляхом машинного навчання та програмне забезпечення для моніторингу та збору даних стану системи пристроїв.

THE MODIFIED INTERNET OF THINGS NETWORK SECURITY SYSTEM

Bushynskyi D.A.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: dbushynskyi2002@gmail.com

As devices improve, computing power increases, and energy consumption decreases, the IoT adoption trend will continue. One of the most difficult topics in this interconnected world of miniature systems and sensors is the aspects of security and privacy: without the assurance that private information is guaranteed to be safe and properly protected, users are reluctant to accept this new technology that seamlessly integrates into life. For IoT to be widely adopted, this issue must be addressed to provide users with confidence in the privacy and control of their personal information.

The specifics of this work include research on solving the problem of protection and privacy through machine learning and software for monitoring and collecting data on the state of the device system.

ПРОБЛЕМИ ОБРОБКИ ГРАФІЧНОЇ ІНФОРМАЦІЇ В МЕРЕЖІ IOT

Любарська С.І.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: lovejapancat1@gmail.com

Досліджено методи обробки графічної інформації в мережі Інтернету речей. Сформовано та проаналізовано перелік проблем що виникають під час обробки графічної інформації, а також способів подолання проблем.

PROBLEMS OF GRAPHIC INFORMATION PROCESSING IN THE IOT NETWORK

Liubarska S.I.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: lovejapancat1@gmail.com

The methods of graphic information processing in the Internet of Things network were studied. A list of problems arising during the processing of graphical information, as well as ways to overcome problems, was formed and analyzed.

ЕНЕРГЕТИЧНЕ ПРОГНОЗУВАННЯ
У ГІБРИДНИХ МІКРОМЕРЕЖАХ

Корнійчук І.Г.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий Інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна
E-mail: korniichuk2002@gmail.com

Інтеграція відновлюваних джерел енергії в мікромережі набрала обертів протягом багатьох років через зростаючий попит та потребу в стійких джерелах енергії. Однак коливання відновлюваних джерел енергії, таких як сонце та вітер, створюють проблему для надійної та ефективної роботи мікромереж. Саме тут енергетичне прогнозування відіграє вирішальну роль у досягненні оптимальної продуктивності мікромережі.

У цій роботі досліджується, як енергетичне прогнозування забезпечує ефективне управління енергією, оптимальне використання відновлюваних джерел та зниження експлуатаційних витрат за допомогою машинного навчання та методів штучного інтелекту.

ENERGY FORECASTING
IN HYBRID MICROGRIDS

Korniichuk I.H.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: korniichuk2002@gmail.com

The integration of renewable energy sources into microgrids has been gaining momentum for many years due to increasing demand and the need for sustainable energy sources. However, fluctuations in renewable energy sources such as the sun and wind create a problem for the reliable and efficient operation of microgrids. This is where energy forecasting plays a crucial role in achieving optimal microgrid productivity.

This work explores how energy forecasting enables effective energy management, optimal utilization of renewable sources, and reduces operational costs through machine learning and artificial intelligence methods.

ТЕНДЕНЦІЇ РОЗВИТКУ РАДІОРЕЛЕЙНИХ СИСТЕМ

Кравченко І.М.
Науковий керівник: **Наритник Т.М.**
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: il.kravchenko115@gmail.com

Досліджено тенденції розвитку радіорелейних систем. Розглянуто революційну радіостанцію “точка-точка” AirFiber від компанії Ubiquiti. Розробка особливого внутрішньо-фірмового протоколу AirMax, за допомогою якого ведеться бездротова передача даних. Перехід радіорелейних систем на більш високі частоти. Перехід до автоматизації та дистанційного керування в радіорелейних системах.

TRENDS IN THE DEVELOPMENT OF RADIO RELAY SYSTEMS

Kravchenko I.M.
Scientific adviser: **Narytnyk T.M.**
Educational and Scientific Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: il.kravchenko115@gmail.com

The trends in the development of radio relay systems are studied. The revolutionary point-to-point radio station AirFiber from Ubiquiti is considered. The development of a special intra-company protocol AirMax, which is used for wireless data transmission. Migration of radio relay systems to higher frequencies. Transition to automation and remote control in radio relay systems.

ПРОБЛЕМИ ВІРТУАЛІЗАЦІЇ В МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ

Сахнюк О.Р.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: tgcsdbdgfc@gmail.com

Інтернет речей стрімко розвивається в наші дні. При цьому на перший план виступає проблема підвищення ефективності такої мережі. В даній публікації для підвищення ефективності запропоновано застосування технології віртуалізації. В рамках дослідження проаналізовано проблематику фізичного обладнання, затримки в обробці даних, проблеми масштабованості та безпеки тощо. На основі проведеного аналізу сформовано перелік рекомендацій щодо застосування технології віртуалізації в мережі Інтернету речей.

PROBLEMS OF VIRTUALIZATION ON THE INTERNET OF THINGS NETWORK

Sakhniuk O.R.
Scientific supervisor: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: tgcsdbdgfc@gmail.com

The Internet of Things is developing rapidly these days. At the same time, the problem of increasing the efficiency of such a network comes to the fore. In this publication, the use of virtualization technology is proposed to increase efficiency. The study analyzes the problems of physical equipment, delays in data processing, scalability and security issues, etc. The list of recommendations for the use of virtualization technology on the Internet of Things network has been formed.

ПОРІВНЯННЯ МЕТОДІВ ЗБОРУ ТА ОБРОБКИ ІНФОРМАЦІЇ В СЕНСОРНІЙ МЕРЕЖІ

Петровський Д. С.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: dimiggptr@gmail.com

В публікації проведено порівняння методів збору та обробки інформації у сенсорних мережах. Одним із ключових факторів, який слід враховувати під час збору даних, є компроміс між точністю та ефективністю. Синхронізація часу є ще одним серйозним викликом у зборі та обробці даних, особливо у великомасштабних сенсорних мережах. Окремим критичним фактором є безпека. З урахуванням проаналізованих факторів в публікації окремо проаналізовано ефективність централізованих та розподілених методів збору та обробки інформації.

COMPARISON OF METHODS FOR DATA COLLECTION AND PROCESSING IN SENSOR NETWORK

Petrovskyi D.S.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: dimiggptr@gmail.com

The publication compares the methods of collecting and processing information in sensor networks. One of the key factor of the data collection is the compromise between accuracy and efficiency. Synchronization is another major challenge in data acquisition and processing, especially in large-scale sensor networks. A separate critical factor is security. Taking into account the analyzed factors, the publication separately analyzes the effectiveness of centralized and distributed methods of information collection and processing.

АНАЛІЗ ПРОБЛЕМИ МАСШТАБОВАНОСТІ МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ

Ткаченко В.М.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: vitalik26tkachenko@gmail.com

Збільшення популярності Інтернету речей є важливим аспектом сьогодення, з метою спростити життя в кожному куточку з'являється все більше різноманітних пристроїв. Однією з основних проблем мережі Інтернету речей є проблема масштабованості, на аналіз та вирішення якої направлена дана публікація. Зокрема проаналізовано здатність управління системою при збільшенні кількості пристроїв в ній, та на основі проведеного аналізу сформовано рекомендації щодо процесу масштабованості мережі.

SCALABILITY PROBLEM OF IOT NETWORK

Tkachenko V.M.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: vitalik26tkachenko@gmail.com

The growing popularity of the Internet of Things is an important aspect of today's world, with more and more devices appearing in every corner to simplify life. One of the main problems of the Internet of Things network is the scalability problem, which this publication is aimed at analyzing and solving. In particular, we analyze the ability to manage the system with an increase in the number of devices in it, and based on the analysis, we formulate recommendations for the network scalability process.

МЕРЕЖА ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ КЕРУВАННЯ ДОРОЖНІМ РУХОМ

Лагода А.В.
Науковий керівник: **Носков В. І.**
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: anastasialahoda@gmail.com

Досліджено передачу даних технології Інтернету речей в рамках концепції «Smart City» та розглянуто протоколи Bluetooth, Wi-Fi, Zigbee, ZWave.

A NETWORK OF IOT DEVICES FOR TRAFFIC MANAGEMENT

Lahoda A.V.
Scientific adviser: **Noskov V.I.**
Educational and Scientific Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: anastasialahoda@gmail.com

The data transmission of the Internet of Things technology within the framework of the "Smart City" concept is investigated. Bluetooth, Wi-Fi, Zigbee, ZWave protocols are considered.

МЕТОД КОНТРОЛЮ ЯКОСТІ ЗВ'ЯЗКУ В МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ НА ОСНОВІ БЕЗПРОВОДОВИХ ТЕХНОЛОГІЙ

Мельник В.В.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: melnykv123@gmail.com

Досліджено особливості контролю якості мережі Інтернету Речей (IoT), що є однією з ключових технологій майбутнього. У роботі проведений аналіз існуючих методів контролю якості в IoT-мережах, визначені їхні переваги та недоліки. Запропоновано модифікований метод контролю якості мережі Інтернету Речей, який враховує специфіку IoT-мереж та покращує ефективність контролю якості. Виконано експериментальну перевірку модифікованого методу контролю якості в IoT-мережах.

THE METHOD OF MONITORING THE QUALITY OF THE INTERNET OF THINGS NETWORK BASED ON WIRELESS TECHNOLOGIES

Melnyk V.V.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mailmelnykv123@gmail.com

Investigated the peculiarities of quality control of the Internet of Things (IoT) network, which is one of the key technologies of the future, have been studied. The work analyzes the existing methods of quality control in IoT networks, identifies their advantages and disadvantages. A modified method of quality control of the Internet of Things network is proposed, which takes into account the specifics of IoT networks and improves the effectiveness of quality control. Experimental verification of the modified method of quality control in IoT networks was performed.

МЕТОД АУДИТУ ІНФОКОМУНІКАЦІЙНОЇ МЕРЕЖІ ВЕЛИКИХ ПІДПРИЄМСТВ

Ковальська Д.Д.
Науковий керівник: **Курдеча В.В.**
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: darinakovalskaaa@gmail.com

Метод аудиту інфокомунікаційної мережі великих підприємств є невід'ємною частиною управління інфраструктурою та її безпекою. Він включає в себе збір та аналіз даних про стан мережі, перевірку її стійкості до зовнішніх загроз та інші важливі процеси.

Модернізація методів аудиту інфокомунікаційної мережі є необхідною для забезпечення безперебійної роботи великих підприємств. Сучасні технології дозволяють автоматизувати процеси збору та обробки даних, що забезпечує високу достовірність результатів та скорочення часу на проведення аудиту. Впровадження нових методів аудиту допоможе підприємствам ефективніше використовувати ресурси.

THE METHOD OF AUDITING THE INFORMATION COMMUNICATION NETWORK OF LARGE ENTERPRISES

Kovalska D.D.
Scientific adviser: **Kurdecha V.V.**
Educational and Scientific Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: darinakovalskaaa@gmail.com

The method of auditing the information communication network of large enterprises is an integral part of infrastructure management and its security. It includes the collection and analysis of data about the state of the network, checking its resistance to external threats and other important processes.

Modernization of information communication network audit methods is necessary to ensure smooth operation of large enterprises. Modern technologies make it possible to automate the processes of data collection and processing, which ensures high reliability of results and shortens the time for conducting an audit. Implementation of new audit methods will help enterprises to use resources more efficiently.

ПЕРСПЕКТИВИ РОЗВИТКУ ТЕХНОЛОГІЇ FIREWALL У КОНТЕКСТІ РОЗВИТКУ ГЛОБАЛЬНОЇ МЕРЕЖІ ТА ЗРОСТАННЯ ОБ'ЄМУ ІНФОРМАЦІЇ

Кириндась Н.П.
Науковий керівник: **Валуйський С.В.**
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: pixelonlline@gmail.com

З ростом та поширенням складних кіберзагроз і атак технологія Firewall стала важливим інструментом для забезпечення мережевої безпеки. У дослідженні розглядається еволюція технології Firewall та її поточний стан у вирішенні проблем сучасної цифрової епохи. Крім того, дослідження розглядає потенційні розробки та досягнення технологій брандмауерів, які можуть ефективно захистити мережі та захистити від нових кіберзагроз. Також висвітлюються значення технології Firewall як невід'ємного компонента мережевої безпеки та її потенційну роль у формуванні майбутнього інформаційної безпеки.

PROSPECTS OF FIREWALL TECHNOLOGY DEVELOPMENT IN THE CONTEXT OF GLOBAL NETWORK DEVELOPMENT AND INFORMATION VOLUME GROWTH

Kyryndas N.P.
Scientific adviser: Valuiskyi S.V.

Educational and Scientific Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: pixelonlline@gmail.com

With the rise of sophisticated cyber threats and attacks, Firewall technology has become an essential tool for ensuring network security. This paper delves into the evolution of Firewall technology and examines its current state in addressing the challenges of the modern digital landscape. Additionally, the research discusses the potential developments and advancements of Firewall technology that can effectively secure networks and protect against emerging cyber threats. Also, the paper highlights the significance of Firewall technology as an integral component of network security and its potential role in shaping the future of information security.

ТЕСТУВАННЯ ТА ІМПЛЕМЕНТАЦІЯ ТЕХНОЛОГІЇ СУПУТНИКОВОГО ЗВ'ЯЗКУ STARLINK У СУЧАСНИХ УМОВАХ ВИКОРИСТАННЯ

Лісовський К.С.
Науковий керівник: **Живков О.П.**
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: k.lisovskyi-2024@kpi.ua

Робота має на меті дослідити ефективність Starlink у забезпеченні надійних та безпечних комунікаційних можливостей у складних бойових умовах. Дослідження буде оцінювати продуктивність Starlink з точки зору його пропускної здатності, затримки та інших відповідних параметрів в таких умовах. Аналіз впливу факторів навколишнього середовища, таких як погода і місцевість, на продуктивність Starlink в бойових ситуаціях.

TESTING AND IMPLEMENTATION OF STARLINK SATELLITE COMMUNICATION TECHNOLOGY IN CONDITIONS OF USE

Lisovskyi K.S.
Scientific adviser: **Zhivkov A.P.**
Educational and Scientific Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: k.lisovskyi-2024@kpi.ua

The study aims to investigate the effectiveness of Starlink in providing reliable and secure communication capabilities in challenging combat environments. The research will evaluate the performance of Starlink in terms of its bandwidth, latency, and other relevant parameters in such conditions. Additionally, the study will also analyze the impact of environmental factors, such as weather and terrain, on the performance of Starlink in combat situations.

РОЗРАХУНОК ТА ПРАКТИЧНА ПЕРЕВІРКА ЗАВАД ПЕРЕДАЧІ ДАНИХ У СИСТЕМІ СУПУТНИКОВОГО ЗВ'ЯЗКУ STARLINK В УМОВАХ СУЧАСНОГО ВИКОРИСТАННЯ

Шелест Є.В.
Науковий керівник: **Живков О.П.**
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: krohaenot522@gmail.com

У роботі використовуються математичні моделі та методи аналізу спектральних характеристик сигналу для оцінки можливих завад, що можуть виникнути в системі під час її використання в умовах бойових дій. Перевірка отриманих результатів проводиться шляхом експериментального дослідження на термінальному обладнанні Starlink з використанням імітації реальних умов "бойового" використання. Отримані результати дослідження можуть бути використані для покращення ефективності та надійності системи супутникового зв'язку Starlink під час використання в умовах бойових дій.

CALCULATION AND PRACTICAL CHECK OF DATA TRANSMISSION OBSTRUCTIONS IN STARLINK SATELLITE COMMUNICATION SYSTEM UNDER THE CURRENT TERMS USE

Shelest Y.V.
Scientific adviser: **Zhivkov A.P.**
Educational and Scientific Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: krohaenot522@gmail.com

The work uses mathematical models and methods for analyzing the spectral characteristics of the signal to assess the possible interference that may arise in the system during its use in combat. Verification of the results obtained is carried out by experimental research on Starlink terminal equipment using simulation of real conditions of "combat" use. The results of the study can be used to improve the efficiency and reliability of the Starlink satellite communication system during use in combat situations.

POTENTIAL DEVELOPMENT & IMPLEMENTING OF BLOCKCHAIN AND CRYPTOCURRENCIES IN THE EUROPEAN UNION AND THE EUROZONE (INCLUDING UKRAINE)

Kostiantyn Lisovskyi[1], Gleb-David Rochenovich[2]
Scientific adviser: Dr. Muhammad Rizky Prima Sakti
[1]*Educational and Scientific Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine*
[2]*Department of Business Administration University College of Bahrain (UCB), Kingdom of Bahrain*
E-mail: androgleb@gmail.com

This paper aims to investigate the potential development and implementation of blockchain and cryptocurrencies in the European Union and the Eurozone. We provide an overview of the technology behind blockchain and cryptocurrency, as well as the potential roles they can play in the European Union and the Eurozone. We then discuss the potential benefits and challenges associated with the development and implementation of such technologies. We conclude by discussing the implications of blockchain and cryptocurrency for the European Union and the Eurozone.

ПОТЕНЦІАЛ РОЗВИТКУ ТА ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ТА КРИПТОВАЛЮТИ В ЄВРОПЕЙСЬКОМУ СОЮЗІ ТА ЄВРОЗОНІ (ВКЛЮЧАЮЧИ УКРАЇНУ)

Костянтин Лісовський, Гліб-Давид Рошеновіч
Науковий керівник: **проф. Мухаммад Різки Пріма Сакті**
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
Факультет бізнес-адміністрування Університетського коледжу Бахрейну (UCB), кор-во Бахрейн
E-mail: androgleb@gmail.com

Робота спрямована на дослідження потенційного розвитку та впровадження блокчейну та криптовалют у Європейському Союзі та у Єврозоні. Пропонується огляд технології, що лежить в основі блокчейну та криптовалюти, а також потенційну роль, яку вони можуть відігравати в Європейському Союзі та у Єврозоні. Обговорюються потенційні переваги та проблеми, пов’язані з розробкою та впровадженням даних технологій в Україні. Як висновок – доцільність впровадження даної технології, а також наслідки даної системи у ЄС та ЄЗ.

APPLYING THE MARSHALL PLAN TO UKRAINE'S ECONOMIC RECOVERY AFTER THE WAR

Mykhaylo Gavryliv
Scientific adviser: **Prof. John Wetherell**
Faculty of European University EU Business School, Spain
E-mail: gavryliv03@gmail.com

This study examines the application of the Marshall Plan to Ukraine's economic recovery after the war. The purpose of the study was to establish how effective this Marshall Plan would be. Interviews were also conducted to determine the extent to which Ukrainian enterprises and techno companies have adapted to wartime conditions. What are the prospects for accession to the European Union? What innovative technologies can Ukraine get, and what can it give in return? The interview information revealed positive signs supporting these hypotheses for the current period. As the war is not over yet, but the positive results are already there, the author presents an analysis of the work done as of December 22, 2022.

ЗАСТОСУВАННЯ ПЛАНУ МАРШАЛЛА ДЛЯ ВІДНОВЛЕННЯ ЕКОНОМІКИ УКРАЇНИ ПІСЛЯ ВІЙНИ

Михайло Гаврилів
Науковий керівник: **проф. Джон Везрелл**
Європейський університет Бізнес-школи ЄС, Іспанія
E-mail: gavryliv03@gmail.com

У цьому дослідженні розглядається застосування плану Маршалла для економічного відновлення України після війни. Метою дослідження було визначити, наскільки ефективним буде цей план Маршалла. Також були проведені інтерв’ю, щоб визначити, наскільки українські підприємства та технологічні компанії адаптувалися до умов війни. Які перспективи вступу до Євросоюзу? Які інноваційні технології Україна може отримати і що може дати натомість? Інформація з інтерв'ю виявила позитивні ознаки, що підтверджують ці гіпотези на поточний період. Оскільки війна ще не закінчилася, але позитивні результати вже є, автор наводить аналіз виконаної роботи станом на 22 грудня 2022 року.