



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

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ
НДІ ТЕЛЕКОМУНІКАЦІЙ**

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

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

15–19 квітня 2024 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**

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

and

**Sixteenth international Scientific Conference of undergraduate and
graduate students "PROSPECTS FOR DEVELOPMENT OF
INFORMATION-TELECOMMUNICATION
TECHNOLOGIES AND SYSTEMS"**

April 15-19, 2024

Conference proceedings

Kyiv

XVIII Міжнародна науково-технічна конференція "Перспективи телекомунікацій" ПТ-2024: Збірник матеріалів конференції. К.: КПІ ім. Ігоря Сікорського, 2024. – с.331.

XVIII International Scientific Conference "Modern Challenges in Telecommunications" MCT-2024. Conference proceedings. Kyiv. Igor Sikorsky Kyiv Polytechnic Institute, 2024 – p. .331.

XVI Міжнародна науково-технічна конференція студентів та аспірантів «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем» ПРІТС 2024: Збірник тез конференції. К.: КПІ ім. Ігоря Сікорського, 2024.

Збірник містить матеріали пленарних і секційних доповідей, представлених на Вісімнадцятій міжнародній науково-технічній конференції "Перспективи телекомунікацій" (ПТ 2024) та Шістнадцятій міжнародній науково-технічній конференції студентів та аспірантів «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем» (ПРІТС 2024), дати проведення 15–19 квітня 2024 р. в м. Києві.

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

<http://conferenc.its.kpi.ua/proc/issue/archive>

<http://journals.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 телекомунікаціях.
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, Київ.

Члени Програмного комітету "Перспективи телекомунікацій":

АВДЄЄНКО Г.Л. – к.т.н., доц., КПІ ім. Ігоря Сікорського, (6), Київ;

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., доц., 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 VA 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., проф., 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;
ШПЛЬНЕР Йозеф - Dr. at ZHAW School of Engineering, Цюрих, Вінтертур, Швейцарія;
ЯВІСЯ В.С. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
ЯКОРНОВ Є.А. - к.т.н., проф., КПІ ім. Ігоря Сікорського, Київ.

Технічний комітет:

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 I 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 (Пленарні засідання: корпус № 6 зал засідань, м. Київ, пр. Берестейський, 37-е) та дистанційно (за допомогою on-line сервісів для відеоконференцій та вебінарів ZOOM).

ЗМІСТ

Пленарні доповіді

Доповідачі:

Joachim Oberhammer

SUB-THZ AND THZ ANTENNAS FOR FUTURE RADAR AND TERABIT WIRELESS COMMUNICATION (матеріал відсутній).....19

Gintaras Valušis

TERAHERTZ STRUCTURED LIGHT – APPLICATIONS IN IMAGING AND COMMUNICATIONS (матеріал відсутній)20

Maryna Popova

DIGIJD: GERMAN -UKRAINIAN PROJECT "DIGITAL EDUCATION WITH JOINED EFFORTS" (матеріал відсутній).....21

Rina Novogradska

ONTOLOGICAL MODELS. EXPERIENCE OF APPLICATION IN TELECOMMUNICATION SCIENCE INSTITUTE (матеріал відсутній)22

Слободяник В.А., Лисенко О.І.

ВПЛИВ ІННОВАЦІЙ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НА СУЧАСНУ ВІЙНУ23

Pavlos Lazaridis

5G/6G ANTENNA OPTIMIZATION (матеріал відсутній)26

Уривський Л.О., Шмігель Б.О.

ПОРІВНЯННЯ ЕФЕКТИВНОСТІ ШИРОКОСМУГОВИХ ТА ВУЗЬКОСМУГОВИХ СИГНАЛІВ В УМОВАХ НИЗЬКОЇ ЕНЕРГЕТИКИ27

Кононова І.В.

ШТУЧНИЙ ІНТЕЛЕКТ В СФЕРІ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ30

Kostiantyn Lisovskyi

SCIENTIFIC AND PRACTICAL ACTIVITIES STUDENTS OF THE ER ITS (матеріал відсутній).....34

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:

Лівенцев С.П., Созонник Г.Д.

МЕТОД АДАПТИВНОГО УПРАВЛІННЯ ПРОЦЕСОМ
ДЕКОДУВАННЯ ТУРБОПОДІБНИХ КОДІВ 35

Носков В.І.

ОЦІНКА ШВИДКОСНИХ ХАРАКТЕРИСТИК ТЕХНОЛОГІЇ VDSL2-
VECTORING В УМОВАХ ПЕРЕХІДНИХ ЗАВАД 40

Ліла Д.В., Бердников О.М.

ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ DWDM over CWDM В ОПТИЧНИХ
МЕРЕЖАХ ДОСТУПУ 43

Уривський Л.О., Могилевич В.Д.

АНАЛІЗ АТАК В ПРОГРАМНО-КЕРОВАНИХ МЕРЕЖАХ 46

Tysak V., Osypchuk S.

RELIABLE INFORMATION TRANSMISSION IN 3GPP STANDARDS
FOR IOT SOLUTIONS 50

Klishchuk V., Osypchuk S.

INFORMATION TRANSMISSION PROBLEMS IN DUAL-PURPOSE IOT
SOLUTIONS 53

Григоренко О.Г., Дідковська Н.А.

ПРОТОКОЛИ РІВНЯ ЗАСТОСУНКІВ В МЕРЕЖАХ ІоТ 56

Григоренко О.Г., Петренко В.О.

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ ІоТ В ПРОМИСЛОВОСТІ 59

Хрокало О. Г., Мошинська А. В.

РОЗРОБКА СИСТЕМИ ВІДАЛЕНОЇ ДІАГНОСТИКИ АВТОМОБІЛІВ
НА ОСНОВІ ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ..... 62

Голубєва М. А. Мошинська А. В.

РОЗРОБКА СИСТЕМИ ДИСТАНЦІЙНОГО КЕРУВАННЯ
ЕЛЕКТРОМЕРЕЖЕЮ ЖИТЛОВОГО ПРИМІЩЕННЯ НА ОСНОВІ
ТЕХНОЛОГІЙ ІоТ 65

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:

Бушинський Д.А., Романов А.О. ПРОБЛЕМИ АНАЛІЗУ ТРАФІКУ В МЕРЕЖІ ІОТ З ТЕХНОЛОГІЄЮ LI-FI.....	68
Іванов С.В., Олійник П.Б. РОЗПІЗНАВАННЯ ДЕФЕКТІВ НАМОТКИ ВОЛОКОННИХ КОТУШОК ВОГ	71
Galitskiy I., Kamarali R., Shevtsov K., Kirilyuk V. MICROSTRIP 4-RESONATOR FILTERS WITH ATTENUATION POLES	75
Маньківський В.Б., Коршак О.О. ПЕРЕВАГИ ТА НЕДОЛІКИ ВИКОРИСТАННЯ МІКРОСЕРВІСНОГО ПАТТЕРНУ ПРОЕКТУВАННЯ	78
Кравченко М.А., Романов М.О. ПІДВИЩЕННЯ ЯКОСТІ ОБСЛУГОВУВАННЯ В МЕДИЧНІЙ СФЕРІ ЗА РАХУНОК ВИКОРИСТАННЯ DOCKER ТА KUBERNETES	81
Романов О.І., Мікляєв Г.О. ВНУТРІШНЄ ПОЗИЦІОНУВАННЯ ЗА ПОШУКОМ НАЙБЛИЖЧОГО ЗНАЧЕННЯ RSS ВИКОРИСТОВУЮЧИ ТЕХНОЛОГІЮ LI-FI.....	85
Підпалій О.І., Нестеренко М.М. НАДАННЯ ПОСЛУГ SIP-ТРАНКІНГ ЧЕРЕЗ ХМАРНІ SBC	88
Triska N.R. ALIGNMENT JITTER EVALUATION IN DIGITAL TRANSMISSION SYSTEMS USING QUEUING MODEL	91
Trubarov I.V. ULTRA-WIDEBAND MICROWAVE PRINTED MICROSTRIP DISC ANTENNA	94
Trubin A. A. MUTUAL COUPLING COEFFICIENTS BASIC AND HIGHER MODES OF SPHERICAL DIELECTRIC RESONATORS	97
Trubin A. A. PERTURBATION THEORY OF COUPLED OSCILLATION OF RESONATORS WITH ACTIVE AND ABSORBING DIELECTRIC	100

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:

Василенко С. В., Єрохін В. Ф.

СПОСІБ СУМІСНОЇ ПРОСТОРОВО-ЧАСОВОЇ ТА МОДЕМНОЇ
КОМПЕНСАЦІЇ СТРУКТУРНОЇ ЗАВАДИ ЦИФРОВОЇ РАДІОЛІНІЇ
З ШИРОКОСМУГОВИМ ФАЗОМАНІПУЛЬОВАНИМ СИГНАЛОМ103

Авдєєнко Г. Л., Наритник Т. М., Шевцов К. О.

МОДЕЛЮВАННЯ ДІЕЛЕКТРИЧНОЇ РЕЗОНАТОРНОЇ АНТЕНИ
ДІАПАЗОНУ 4 ГГЦ.....106

Якорнов Є.А., Тичинський-Мартинюк В.Ю.

ПОКРАЩЕННЯ ЕФЕКТИВНОСТІ СИМВОЛЬНОГО ПЛАНУВАННЯ
В МЕРЕЖАХ 5G ШЛЯХОМ ЗАСТОСУВАННЯ СУМІСНИХ
СЛОТОВИХ ФОРМАТІВ109

Astrakhtantsev A.A., Hryschuk I.A., Pedan S.I.

ANALYSIS OF THE CHARACTERISTICS OF ROUTING PROTOCOLS
IN AD-HOC NETWORK.....112

Лагода А.В., Трубаров. І.В.

ОПТИМІЗАЦІЙНИЙ ПІДХІД ДО ВИБОРУ ПАРАМЕТРІВ
МІКРОХВИЛЬОВИХ ЛІНІЙ ЗВ'ЯЗКУ ПРЯМОЇ ВИДИМОСТІ115

Правило В.В.

ЗАБЕЗПЕЧЕННЯ ЗАДАНИХ ПОКАЗНИКІВ БЕЗПЕКИ ПЕРЕДАЧІ
ДАНИХ В 4G МЕРЕЖАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ118

Кайденко М.М., Роскошний Д.В.

ВИБІР ОПТИМАЛЬНИХ ПАРАМЕТРІВ ЛЧМ СИГНАЛУ ДЛЯ
КАНАЛІВ ЗВ'ЯЗКУ БПЛА, РЕАЛІЗОВАНИХ НА БАЗІ SDR
ТРАНСИВЕРІВ.....121

Кайденко М.М., Роскошний Д.В.

РЕАЛІЗАЦІЯ УЗГОДЖЕНОГО ФІЛЬТРУ ДЛЯ ЛЧМ СИГНАЛІВ ПРИ
ВИКОРИСТАННІ SDR ТРАНСИВЕРА НА БАЗІ SYSTEM-ON-CHIP.....124

Ветошко І.П., Кравчук С.О.

МЕТОДИ РЕАЛІЗАЦІЇ ТЕХНОЛОГІЇ ПЕРЕДАЧІ ГОЛОСУ VONR У
МЕРЕЖАХ 5G. ОПЦІЇ ДЛЯ ІСНУЮЧИХ ОПЕРАТОРІВ.....127

Кравчук С.О., Кравчук І.М. ПРОЦЕДУРИ АУТЕНТИФІКАЦІЇ ТЕРМІНАЛІВ ТА ПРОМІЖНИХ МОДУЛІВ НА БАЗІ РОЮ БПЛА ЯК ЧАСТИНИ МЕРЕЖІ РАДІОДОСТУПУ 5G	130
Сколець С.С., Кравчук С.О. МЕТОДИ ВІРТУАЛІЗАЦІЇ МЕРЕЖ МОБІЛЬНОГО ЗВ'ЯЗКУ 4G ТА 5G З МЕТОЮ ПІДВИЩЕННЯ ЯКОСТІ ОБСЛУГОВУВАННЯ	133

Секція 4. Інформаційні технології в телекомунікаціях

Співголови:

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

Доповідачі:

Бугайов М.В. АНАЛІЗ РАДІОЧАСТОТНОГО СПЕКТРА ІЗ ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ.....	136
Ільницький А.І., Захарчук Л.В., Цуканов О.Ф. МОДИФІКОВАНИЙ МЕТОД ГЕРЦЕЛЯ - БЛЕЙХУТА ВИЗНАЧЕННЯ ТОНАЛЬНИХ СИГНАЛІВ ПРИ МОНІТОРИНГУ	139
Глоба Л.С., Цуканов О.Ф. ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ТЕЛЕКОМУНІКАЦІЯХ	142
Tovstii A.O., Shumskiy B.S., Sierhieiev V.V., Globa L.S. ONTOLOGY OF DIGITAL COMPUTER ONLINE LEARNING PLATFORM.....	145
Педан С.І., Мельник М.В., Алексєєв М.О. ПІДВИЩЕННЯ БЕЗПЕКИ СПОЛУЧЕННЯ ІОТ ПРИСТРОЇВ ШЛЯХОМ АНАЛІЗУ БЕЗПРОВІДНИХ СИГНАЛІВ	148
Педан С.І., Романович О.Д., Алексєєв М.О. ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ПЕРЕДАЧІ МЕДІА ДАНИХ З ВИКОРИСТАННЯМ ЗАВАДОСТІЙКОГО КОДУВАННЯ.....	152

Шелест Є.В., Алексєєв М.О., Педан С.І. ОГЛЯДОВИЙ АНАЛІЗ ТЕХНОЛОГІЙ КОНТЕЙНЕРИЗАЦІЇ ДЛЯ ВИКОРИСТАННЯ У ГЕТЕРОГЕННОМУ СЕРЕДОВИЩІ ІЗ ДИНАМІЧНОЮ АРХІТЕКТУРОЮ	156
Ковальська Д. Д., Курдеча В.В., Якорнов Є.А. МЕРЕЖЕВИЙ АУДИТ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖ	161
Терещенко В.О., Курдеча В.В. ПРОЦЕС ОНОВЛЕННЯ ПРИСТРОЇВ ІОТ.....	164
Солоденко М.А., Курдеча В.В. ДОСЛІДЖЕННЯ СУЧАСНИХ МЕТОДІВ ЗБОРУ ІНФОРМАЦІЇ ВУЗЛІВ ІНТЕРНЕТУ РЕЧЕЙ	167
Руденко А.А., Курдеча В.В. ВИКОРИСТАННЯ ТЕХНОЛОГІЇ LI-FI В МЕРЕЖІ INTERNET OF THINGS	170
Степанов Г. О., Новогрудська Р. Л. КОМПЛЕКСНИЙ АНАЛІЗ МЕТОДІВ ВИКОРИСТАННЯ СИСТЕМ ЗБЕРІГАННЯ ЕЛЕКТРОЕНЕРГІЇ ДЛЯ MICROGRID	173
Сегеда С.А., Алексєєв М.О., Педан С.І. ПІДХІД ДО БАЛАНСУВАННЯ НАВАНТАЖЕННЯ ВЕБ-СЕРВІСІВ У ГЕТЕРОГЕННОМУ КЛАСТЕРІ НА ОСНОВІ DOCKER SWARM.....	177
Столяр С.В., Комаров І.Ю., Ігнатова С.С. РОЗРОБКА ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ ДЛЯ АВТОМАТИЗАЦІЇ МОНІТОРИНГУ ТА УПРАВЛІННЯ ТРАНСПОРТНОЮ СИСТЕМОЮ МІСТА КИЄВА З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ	180
Радіонов М.Р., Комаров І.Ю., Ігнатова С.С. TELEGRAM - БОТ ДЛЯ РОЗРАХУНКУ ПОДАТКІВ	183
Чубай Д. Р., Ігнатова С.С. ВИЯВЛЕННЯ СИГНАЛІВ БПЛА ЗА ДОПОМОГОЮ НЕЙРОМЕРЕЖ (НА ПРИКЛАДІ НАБОРІВ ДАНИХ КОМЕРЦІЙНИХ ДРОНІВ)	185
Oliinyk D.I., Nizhnyi D.A. THE ROLE OF ARTIFICIAL INTELLIGENCE IN THE FORMATION OF WIRELESS NETWORKS	188

Храбан Д.А., Скулиш М.А.
АНАЛІЗ АЛГОРИТМІВ ДИНАМІЧНОГО КЕРУВАННЯ
РЕСУРСАМИ МЕРЕЖЕВИХ СЛАЙСІВ191

Карташов А.Д., Глоба Л.С.
ОПТИМІЗАЦІЯ У СФЕРІ ЗБЕРІГАННЯ ДАНИХ В ХМАРНИХ
СЕРЕДОВИЩАХ: ПОШУК КОМПЛЕКСНОГО НАБОРУ КРИТЕРІЇВ ...196

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:

Сушин І.О., Лисенко О. І., Авдєєнко Г.Л.
ЗАСТОСУВАННЯ СЕНСОРІВ СПРЯМОВАНОЇ ДІЇ В МОБІЛЬНИХ
БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ199

Тимофєєв Є.М., Лисенко О.І.
ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ КООПЕРАТИВНОГО МІМО ДЛЯ
МІНІМІЗАЦІЇ ЕНЕРГОСПОЖИВАННЯ ПРИ ПЕРЕДАЧІ ДАНИХ В
БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖАХ203

Якорнов Є.А., Цуканов О.Ф.
ПІДВИЩЕННЯ ТОЧНОСТІ ОЦІНЮВАННЯ ПАРАМЕТРІВ РУХУ
НЕВЕЛИКИХ БЕЗПЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ЗА
РАХУНОК ВРАХУВАННЯ ВІТРУ НА ОСНОВІ ВИКОРИСТАННЯ
ДРОБНИХ РЯДІВ ТЕЙЛОРУ206

Лисенко О.І., Фуртат С.О., Фуртат О.В.
МЕТОДИКА СИНТЕЗУ ЦИФРОВИХ РЕГУЛЯТОРІВ ПРЕЦИЗІЙНИХ
ЕЛЕКТРОПРИВОДІВ ДЛЯ СИСТЕМИ ОРІЄНТАЦІЇ І СТАБІЛІЗАЦІЇ
СТЕЖЕННЯ ЗА ОБ'ЄКТАМИ СЕНСОРІВ СПРЯМОВАНОЇ ДІЇ
МОБІЛЬНИХ РОБОТІВ209

Федорова Л.Б., Москвичова К.К.
ЗАСТОСУВАННЯ ВЕЙВЛЕТ-ПЕРЕТВОРЕНЬ В ЗАДАЧАХ
ОБРОБКИ СИГНАЛІВ В СЕНСОРНИХ МЕРЕЖАХ212

Аверкієв Є.О., Правило В.В.
АНАЛІЗ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ З
ПІДТРИМКОЮ DDoS-АТАК В МЕРЕЖАХ ІоТ216

Насвіт Ю.О., Лисенко О.І., Новіков В.І.
ПАРАМЕТРИ ДЛЯ ПОРІВНЯННЯ ТРАДИЦІЙНИХ ПРОТОКОЛІВ
КЛАСТЕРИЗАЦІЇ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ219

Явіся В.С., Лисенко О.І. ВИКОРИСТАННЯ КОНЦЕПЦІЇ РОЗПОДІЛЕНОГО СУПУТНИКА ДЛЯ ПОБУДОВИ КОСМІЧНОГО СЕГМЕНТУ СИСТЕМИ STARLINK	223
Явіся В.С., Лисенко О.І. МЕТОДИ ЕЛЕКТРОЖИВЛЕННЯ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ	226
Романюк В.А., Гримуд А.Г. ПРАВИЛА ПОБУДОВИ ТРАЄКТОРІЇ ПОЛЬОТУ КОМУНІКАЦІЙНОЇ АЕРОПЛАТФОРМИ ДЛЯ ЗБОРУ ДАНИХ З ВУЗЛІВ БЕЗПРОВОДОВОЇ СЕНСОРНОЇ МЕРЕЖІ	229
Коваленко І.Л., Мовчанюк А.В. ВИКОРИСТАННЯ ПІДХОДУ ІОТ ЯК ПЕРСПЕКТИВНИЙ НАПРЯМ РОЗВИТКУ ПЕРВИННОЇ ДІАГНОСТИКИ СТАНІВ ЛЮДИНИ	232
Карпенко М.І., Чумаченко С.М., Мошенський А.О. АРГУМЕНТАЦІЯ ПОЄДНАННЯ БПЛА ТА БСМ ДЛЯ ДИСТАНЦІЙНОГО ЗОНДУВАННЯ НЕБЕЗПЕЧНИХ РЕЧОВИН	237
Корнійчук І.Г., Курдеча В.В. ГРАНИЧНІ ОБЧИСЛЕННЯ В ІНТЕРНЕТІ РЕЧЕЙ: ЛОКАЛЬНИЙ АНАЛІЗ ТА УПРАВЛІННЯ ЕНЕРГІЄЮ	240
Семенко В.В., Лисенко О.І., Гетьман О.В., Новіков В.І., Фуртат О.В. ПРОЦЕДУРА ВИБОРУ ПРОТОКОЛІВ ПЕРЕДАЧІ ІНФОРМАЦІЇ У МОБІЛЬНИХ СЕНСОРНИХ МЕРЕЖАХ НА ОСНОВІ РОЗВ'ЯЗАННЯ МОДЕЛЬНИХ ЗАДАЧ	243
Krylach O., Okhrimenko O., Tsakhlo O., Zhivkov O. SIMULATION OF THE PURCELL EFFECT BY CIRCUIT THEORY METHODS	247
Galitskiy I., Kyryliuk V., Tychynskiy-Martyniuk V., Zhivkov A. METAMATERIAL PROPERTIES OF MICROSTRIP RECTANGULAR RESONATORS	250
Кошмак А.І. ОПТИМІЗАЦІЯ МАРШРУТИЗАЦІЇ В ЛІТАЮЧИХ СЕНСОРНИХ МЕРЕЖАХ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ	253

Славінський Д.Ю., Лисенко О.І., Гетьман О.В, Новіков В.І., Фуртат О.В.	
РОЗВИТОК АЛГОРИТМІВ КЛАСТЕРИЗАЦІЇ В МОБІЛЬНИХ СЕНСОРНИХ МЕРЕЖАХ	256
Буткевич Г.Ю.	
АНАЛІЗ СИСТЕМИ КОНТРОЛЮ ПОЛОЖЕННЯ ДРОНІВ ПІД ЧАС ШОУ	259
Дрегало Б.О.	
РОЗВИТОК МЕТОДІВ КЕРУВАННЯ ЕНЕРГОЗБЕРЕЖЕННЯМ В БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ	262
Федотов К.Ю., Сергієнко М.І., Кирпич М.С., Кононов А., Колошко І.В.	
АНТЕНА ДЛЯ ПОЛЬОВОГО РАДІОЗВ'ЯЗКУ	265
Кожухар І.В., Лисенко О.І., Гетьман О.В, Новіков В.І., Фуртат О.В.	
РОЗВИТОК МЕТОДІВ СИНХРОНІЗАЦІЇ ДЛЯ МОБІЛЬНИХ СЕНСОРНИХ МЕРЕЖ	267
Кравченко І.М., Міночкін Д.А.	
АВТОМАТИЗАЦІЯ РОБОТИ ДАТАЦЕНТРУ З ВИКОРИСТАННЯМ МАШИННОГО НАВЧАННЯ	270
Третяк А.В. Лисенко О.І.	
ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ СТИСКУ ДАНИХ В БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ	273
Маленчик Т.В., Жук С.Я.	
ВИЯВЛЕННЯ СИГНАЛУ РУХОМОЇ ЦІЛІ FMCW РАДАРІМ ПРИ ВІДОМІЙ ПОТУЖНОСТІ ЗАВАДИ	277
Сукало М.Л., Чумаченко С.М.	
ПРОГРАМНО-АПАРАТНИЙ КОМПЛЕКС АДАПТИВНОГО МОНІТОРИНГУ ОБМЕЖЕНОЇ ЕКОСИСТЕМИ	280
Валуйський С.В., Кравчук І.В.	
МЕТОДИ ЗАХИСТУ ВІД АТАК НА ОДНОРАНГОВІ БЛОКЧЕЙН МЕРЕЖІ БІТКОІНА	283
Валуйський С.В., Кисіль А.І.	
МЕТОДИ КЛАСТЕРИЗАЦІЇ В БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ НАСТУПНОГО ПОКОЛІННЯ	286

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

Співголови:

- 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;
- ЯКОРНОВ Є.А. – к.т.н., професор Навчально-наукового Інституту телекомунікаційних систем КПІ ім. Ігоря Сікорського;
- КРАВЧУК І.М. – к.ю.н., доц., Навчально-наукового Інституту телекомунікаційних систем КПІ ім. Ігоря Сікорського;
- КОСОГОР А.В. – в.о. голови студради НН ІТС КПІ ім. Ігоря Сікорського.

Доповідачі:

Муха Р.В. кер. Токар Л.О.

SMART КАЛЕНДАР ДЛЯ ІОТ ПРИЛАДІВ НА ПРИКЛАДІ
ТЕХНОЛОГІЇ MATTER291

Соловйов П.В. кер. Токар Л.О.

КЛАСТЕРИЗАЦІЯ В МЕРЕЖАХ VANET292

Лемешко В.О., Персіков М.А. кер. Єременко О.С.

АНАЛІЗ МАТЕМАТИЧНИХ МОДЕЛЕЙ МАРШРУТИЗАЦІЇ ТА ЇХ
ЗАСТОСУВАННЯ В ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖАХ ..293

Солом'яний М.В., Персіков М.А. кер. Єременко О.С.

ДОСЛІДЖЕННЯ МОДЕЛЕЙ МАРШРУТИЗАЦІЇ ІЗ
ЗАБЕЗПЕЧЕННЯМ НАДІЙНОСТІ ТА ВІДМОВОСТІЙКОСТІ В
ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ.....294

Недоступ Д.М., Персіков М.А.кер. Єременко О.С.

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ВІДМОВОСТІЙКОСТІ
ЗАСОБАМИ МАРШРУТИЗАЦІЇ В ІНФОКОМУНІКАЦІЙНИХ
МЕРЕЖАХ.....295

Персіков А.В., Шестопапов С.С. кер. Єременко О.С.

ДОСЛІДЖЕННЯ ПРОЦЕСУ БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ ДЛЯ
ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ МЕРЕЖ З ВИКОРИСТАННЯМ
ПРОАКТИВНИХ І РЕАКТИВНИХ ПІДХОДІВ.....296

Скомаха М. О. кер. Єременко О.С

ВИКОРИСТАННЯ МЕТОДІВ ШТУЧНОГО ІНТЕЛЕКТУ ПІД ЧАС
РОЗВ'ЯЗАННЯ ЗАДАЧ ОПТИМІЗАЦІЇ ЯКОСТІ
ОБСЛУГОВУВАННЯ В МЕРЕЖАХ 6G.....297

Солоденко М.А. кер. Курдеча В.В. АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ЗБОРУ ІНФОРМАЦІЇ ВУЗЛІВ ІНТЕРНЕТУ РЕЧЕЙ.....	298
Терещенко В.О. кер. Курдеча В.В. ОСОБЛИВОСТІ ОНОВЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В ПРИСТРОЯХ ІНТЕРНЕТУ РЕЧЕЙ.....	299
Радуга Н.С. Прудкий В.С. кер. Курдеча В.В. МОЖЛИВОСТІ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ НА ФІЗИЧНОМУ РІВНІ У ТЕЛЕКОМУНІКАЦІЯХ.....	300
Пінчук Ю.М. кер. Курдеча В.В. ВПЛИВ СОЦІАЛЬНИХ МЕДІА НА СПРИЙНЯТТЯ ІНФОРМАЦІЇ.....	301
Бех В.О., Касіч Н.Ю. кер. Курдеча В.В. ТЕНДЕНЦІЇ РОЗВИТКУ ОПТОВОЛОКОННИХ ТЕХНОЛОГІЙ	302
Поковба О.Ю. кер. Курдеча В.В. БЕЗДРОТОВІ ТЕХНОЛОГІЇ ПЕРЕДАЧІ ДАНИХ НА ВЕЛИКІ ВІДСТАНІ В МЕРЕЖАХ ІНТЕРНЕТУ РЕЧЕЙ	303
Юсин І. С. кер. Курдеча В.В. ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ ВИЯВЛЕННЯ НАДЗВИЧАЙНИХ СИТУАЦІЙ	304
Чудо А.Р. кер. Курдеча В.В. МОДИФІКОВАНИЙ МЕТОД ЗАХИСТУ КІНЦЕВИХ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ.....	305
Колосовський Д.О. кер. Курдеча В.В. ОСОБЛИВОСТІ УПРАВЛІННЯ ПРИСТРОЯМИ ІНДУСТРІАЛЬНОГО ІНТЕРНЕТУ РЕЧЕЙ.....	306
Закревський М.М. кер. Курдеча В.В. ПРИНЦИП ПОБУДОВИ GRON ТА СУМІЖНИХ ГРУП ОПТОВОЛОКОННИХ ТЕХНОЛОГІЙ	307
Терещенко В.В. кер. Курдеча В.В. ІННОВАЦІЇ ШТУЧНОГО ІНТЕЛЕКТУ В ТЕЛЕКОМУНІКАЦІЙНІЙ ІНДУСТРІЇ	308
Шишкіна С.О., Коба А.О., Книр Г.А. кер. Курдеча В.В. ТЕНДЕНЦІЇ РОЗВИТКУ СТІЛЬНИКОВОГО ЗВ'ЯЗКУ	309

Кузнецов Я.В. кер. Курдеча В.В. ПІДВИЩЕННЯ БЕЗПЕКИ В ІОТ ЗА ДОПОМОГОЮ МЕТОДІВ МАШИННОГО НАВЧАННЯ	310
Журба І.О. кер. Курдеча В.В. ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ В СФЕРІ КОМЕРЦІЙНОЇ ТОРГІВЛІ.....	311
Голуб А.С. кер. Курдеча В.В. РОЗВИТОК ТА ІНТЕГРАЦІЯ ТЕХНОЛОГІЙ 6G ДЛЯ МАЙБУТНЬОГО ПОКОЛІННЯ МОБІЛЬНОГО ЗВ'ЯЗКУ.....	312
Руденко А.А. кер. Курдеча В.В. МОЖЛИВОСТІ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ LI-FI В МЕРЕЖІ INTERNET OF THINGS	313
Нечипоренко А.С. кер. Курдеча В.В. МОДИФІКОВАНА МОДЕЛЬ КОРПОРАТИВНОЇ МЕРЕЖІ ЗВ'ЯЗКУ ..	314
Посвистьол В.В. кер. Курдеча В.В. СУПРОВОДЖЕННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ БАНКІВСЬКОЇ УСТАНОВИ.....	315
Корнійчук І.Г. кер. Курдеча В.В. ОПТИМІЗАЦІЯ ЕНЕРГОПОСТАЧАННЯ ТА СПОЖИВАННЯ ЧЕРЕЗ СТАТИСТИЧНИЙ АНАЛІЗ ДАНИХ.....	316
Тичинський - Мартинюк В.Ю. кер. Якорнов Є.А. ОЦІНКА СУМІСНОСТІ СЛОТОВИХ ФОРМАТІВ СИГНАЛУ В МЕРЕЖАХ 5G	317
Ковальська Д.Д. кер. Якорнов Є.А. УДОСКОНАЛЕННЯ ІНФОКОМУНІКАЦІЙНОГО АУДИТУ	318
Оленюк М.М. кер. Курдеча В.В. АНАЛІЗ СИСТЕМ РОЗУМНОГО БУДИНКУ ДЛЯ ЛЮДЕЙ З ОБМЕЖЕНИМИ МОЖЛИВОСТЯМИ	319
Гінзбург А. , Ігнатова С.С. кер. Комаров І.Ю. ЗАСТОСУВАННЯ ІТ ІНСТРУМЕНТІВ У ПОШУКУ МОНЕТ	320
Обозовий І.Ю., Ігнатова С.С. кер. Комаров І.Ю. СТВОРЕННЯ ТА ЗАСТОСУВАННЯ ТЕЛЕГРАМ БОТУ “RECOMMENDIFY”	321

Хіхло В.Ю. кер. Тверитникова О.Є. РОЗВИТОК ПРОГРАМНО-АПАРАТНИХ ЗАСОБІВ ВИМІРЮВАННЯ В УКРАЇНІ (ДРУГА ПОЛОВИНА ХХ СТ.)	322
Омельченко С.А. кер. Якорнов Є.А. РОЗРОБКА АЛГОРИТМУ АВТОКОМПЕНСАЦІЇ САМОІНТЕРФЕРЕНЦІЙНИХ СИГНАЛІВ В АНТЕНОХВИЛЕВОДНОМУ ТРАКТІ КАНАЛУ ПРИЙОМУ ДЛЯ ОДНОЧАСТОТНИХ СИСТЕМ РАДІОРЕЛЕЙНОГО ЗВ'ЯЗКУ	323
Майба М.А. кер. Єременко О.С. ДОСЛІДЖЕННЯ МЕТОДІВ ІНТЕЛЕКТУАЛЬНОЇ МАРШРУТИЗАЦІЇ В ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖАХ.....	324
Іванова Т.С. кер. Уривський Л.О. АНАЛІЗ ШЛЯХІВ ЕФЕКТИВНОГО ЗАХИСТУ СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ ВІД КІБЕРЗАГРОЗ.....	325
Кравченко І.М. кер. Міночкін Д.А. МАШИННЕ НАВЧАННЯ У АВТОМАТИЗАЦІЇ РОБОТИ ДАТАЦЕНТРУ	326
Третяк А.В. кер. Лисенко О.І. МЕТОДИ СТИСКУ ДАНИХ В БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ.....	327
Мінжинер Н.М. кер. Якорнов Є.А. РОЗРОБКА СИСТЕМИ ЦИФРОВОГО РАДІОРЕЛЕЙНОГО ЗВ'ЯЗКУ ПІДВИЩЕНОЇ ПРОПУСКНОЇ ЗДАТНОСТІ НА ОСНОВІ ЗАСТОСУВАННЯ СФЕРИЧНОСТІ ФРОНТУ ЕЛЕКТРОМАГНІТНОЇ ХВИЛІ В ЗОНІ ФРЕНЕЛЯ.....	328
Скомаха М. О. кер. Єременко О.С МЕТОДИ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ТА ЦІЛІСНОСТІ ІНФОРМАЦІЇ В МЕРЕЖІ 5G МІЛІМЕТРОВОГО ДІАПАЗОНУ	329
Ковальов А.В. кер. Курдеча В.В. ТЕНДЕНЦІЇ РОЗВИТКУ СИСТЕМ ДОСТУПУ BLUETOOTH ТА WI-FI..	330
Косогор А.В. кер. Уривський Л.О. ДОСЛІДЖЕННЯ ПИТАННЯ ЕФЕКТИВНОСТІ ТА ВИПРАВНОЇ ЗДАТНОСТІ КОДІВ РІДА-СОЛОМОНА	331

Пленарні доповіді

**SUB-THZ AND THZ ANTENNAS FOR FUTURE
RADAR AND TERABIT WIRELESS COMMUNICATION**

Joachim Oberhammer

*KTH Royal Institute of Technology School of
Electrical Engineering, Stockholm, Sweden*

**SUB-THZ ТА THZ АНТЕНИ ДЛЯ МАЙБУТНЬОГО
РАДАРІВ ТА ТЕРАБІТНОГО БЕЗДРОТОВОГО ЗВ'ЯЗКУ**

**TERAHERTZ STRUCTURED LIGHT –
APPLICATIONS IN IMAGING AND COMMUNICATIONS**

Gintaras Valušis

Center for Physical Sciences and Technology, Vilnius, Lithuania

**ТЕРАГЕРЦОВЕ СТРУКТУРОВАНЕ СВІТЛО –ЗАСТОСУВАННЯ
В ОБРОТКІ ЗОБРАЖЕНЬ ТА КОМУНІКАЦІЇ**

DIGIJED: GERMAN -UKRAINIAN PROJECT
DIGITAL EDUCATION WITH JOINED EFFORTS"

Maryna Popova

*Communication Systems Department, Hochschule
Anhalt University of Applied Science, Köthen, Germany*

**ONTOLOGICAL MODELS. EXPERIENCE OF APPLICATION IN
TELECOMMUNICATION SCIENCE INSTITUTE**

Rina Novogrudska

*Educational and Scientific Institute of Telecommunication
Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine*

ВПЛИВ ІННОВАЦІЙ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НА СУЧАСНУ ВІЙНУ

Слободяник В.А.¹, Лисенко О.І.²

¹ *Центральний науково-дослідний інститут озброєння та
військової техніки Збройних Сил України,*

² *Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського*

E-mail: Slobol9dianyuk64@ukr.net; Lysenko.a.i.1952@gmail.com

IMPACT OF INNOVATIONS AND INFORMATION TECHNOLOGIES ON MODERN WAR

The life cycle of weapons and the influence of modern innovations and technologies on their development (modernization) are considered. It is shown that the duration of the arms development cycle is constantly decreasing. It has been noted that the modern battlefield is increasingly becoming a battlefield of autonomous and remote-controlled drones.

Сучасне поле бою українсько-російської війни можливо порівняти одночасно з величезним тривимірним полігоном під відкритим небом та дослідною лабораторією випробувань нових технологій. На цьому полігоні одночасно проходять десятки, а іноді і сотні бойових зіткнень, рознесених у просторі і часі. В цих зіткненнях беруть участь окремі елементи і системи різного рівня призначення, складності та технологічності. Результат цих зіткнень (взаємодій) являє собою до певної міри випадкову величину, що залежить від багатьох чинників, зокрема захищеності учасників зіткнень, їх технологічності, прийнятих ними стратегій дій, масовості (кількості учасників кожної зі сторін зіткнення – ефект диференційних рівнянь Ланчестера), і нарешті від зовнішніх факторів, як то погодні та фізико-географічні умови, стан місцевості та її фортифікаційне обладнання (наявність шляхів постачання, їх стан, стан та складність системи укріплень, наявність, щільність та протяжність мінних полів, тощо). Тому можемо говорити тільки про математичне очікування наслідків конфліктної взаємодії двох складних систем різного складу і розмірності. Так, виходячи з наявної інформації, успішне застосування FPV дронів (тобто ураження ними вибраних оператором цілей) сягає приблизно 30% [1]. Тобто у нашій «польовій лабораторії» тільки в трьох бойових зіткненнях з десяти застосування FPV дрона є успішним. І це є результатом багатьох умов, що склалися на той момент, але перш за все технологічності озброєння, навченості оператора та впливу засобів протидії.

Як показує досвід сучасних воєн, військові технології та швидкість їх розробки і застосування є все більш домінуючими на сучасному полі бою [2]. Під військовими технологіями ми розуміємо сукупність методів (способів) виробництва нових зразків озброєння та військової техніки з заданими технічними характеристиками.

Новим технологіям передують нові ідеї – інновації. Під військовими інноваціями будемо розуміти втілення наукового відкриття, технічного винаходу в новій технології або новому виді виробу (Й. Шумпетер) з метою розробки та виробництва нової зброї. Іншими словами інновація – це ідея, яка базується на нових наукових знаннях з метою їх практичного застосування у військовій справі. Взаємозв'язок між інноваціями, технологіями і новою зброєю схематично представлено на Рис.1.

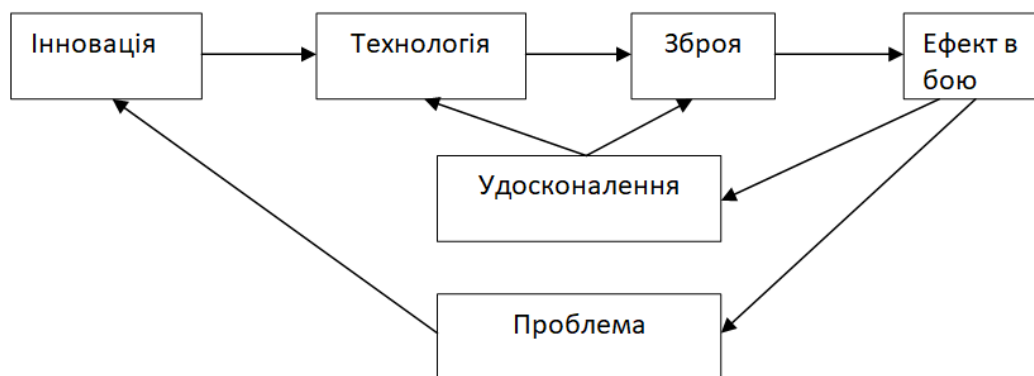


Рис.1. Зв'язок між інноваціями, технологіями і новими зразками зброї.

На Рис.2 представлено життєвий цикл зброї від появи її на полі бою і до заміни на більш сучасні, або модернізовані аналоги.

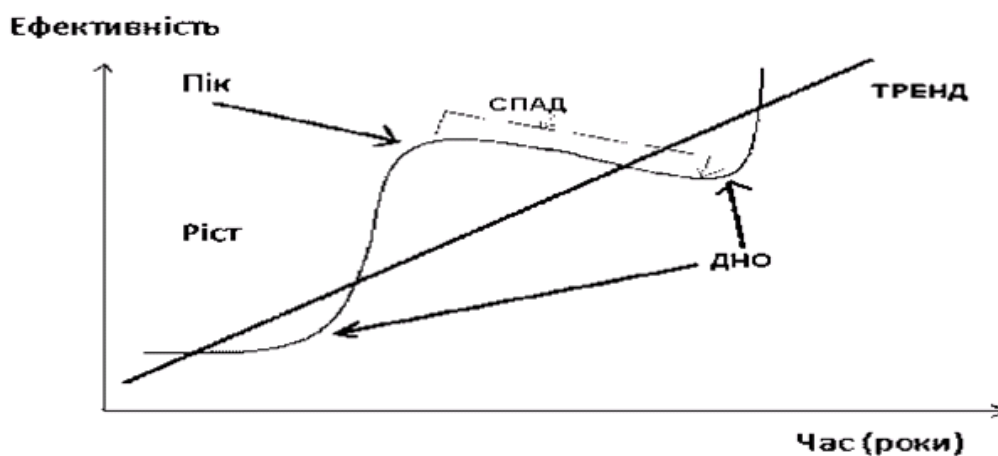


Рис. 2. Життєвий цикл зброї по аналогії з бізнес-циклом в економіці.

Як видно з Рис. 2 період росту ефективності на полі бою, що пов'язаний з освоєнням нової зброї і відпрацюванням нових тактик її застосування в бою, змінюється спадом. Спад пов'язаний з розробкою нових засобів протидії даному зразку зброї. Нова хвиля росту відбувається завдяки модернізації або розробці нового зразка, що перевершують тактико-технічні характеристики існуючого, або ж створенню принципово нового зразка, що приходить на заміну існуючому. Прикладами переходу на принципово-нові зразки зброї є лук - гвинтівка, важка кавалерія – танк, гелікоптер – мультикоптер, тощо. При цьому знижується співвідношення вартості зразка до його бойового потенціалу:

$$\frac{C_i}{\Psi_i} \rightarrow \min_{\forall i \in I} \quad (1)$$

де C_i – вартість i -го зразка-аналога, Ψ_i – бойовий потенціал зразка. Крім того, зменшується інтервал часу, протягом якого проходить такий перехід. Так перехід від лука до гвинтівки зайняв приблизно 13 – 13,5 тисяч років, перехід від важкої кавалерії до танків – приблизно 2,5 тисячі років, а від гелікоптера до дистанційно-керованого мультикоптера – приблизно 80 років.

Нині спостерігаються наступні тенденції у розвитку зразків озброєння та військової техніки: інтелектуалізація, мініатюризація, зниження помітності, підвищення точності, можливість масового виробництва, адаптивні та самоорганізуючі функції, зниження енергоємності, мінімізація часу на виконання завдань, підвищення стійкості до впливу факторів поля бою [3,4].

Поле бою стає все більш складним, швидкоплинним, технологічним, з переходом до домінування автономних та дистанційно-керованих машин. Людині на такому полі бою все більш складно вижити. Автоматизовані та автоматичні, дистанційно-керовані та автономні, з елементами штучного інтелекту безлюдні машин та системи швидко витісняють людину з поля бою. Ці машини та системи мають різне функціональне призначення, і пов'язані між собою складними мережами зв'язку для керування та обміну інформацією.

Нині будь-яка високотехнологічна система озброєння фактично є розподіленою мережею з підсистемами збору інформації, її аналізу та обробки, прогнозування ситуації, підтримки прийняття управлінських рішень, розподілу та ураження виявлених цілей. Основними критеріями оптимальності функціонування таких систем є співвідношення вартості до бойового потенціалу (1) та мінімізації часу на виконання поставлених завдань.

Масоване впровадження нових, високотехнологічних бойових систем кардинально міняє сучасне поле бою, ставлячи нові питання по оптимальному рівню їх адаптивності та самоорганізації, автономності, структурі та функціям окремих елементів таких систем в рамках єдиної глобальної військової мережі, яка бере участь у військовому конфлікті.

Література

1. Станіслав Стрілець Ціль уражено. Як працюють оператори дронів-камікадзе. Репортаж [Електронний ресурс]. – Режим доступу: <https://texty.org.ua/articles/110641/cil-vrazhenovyuzid-na-zavdannya-z-operatoramy-droniv-kamikadze/> – Заголовок з екрану.
2. Rajeswari Pillai Rajagopalan and Sameer Patil, eds, Future Warfare and Critical Technologies: Evolving Tactics and Strategies // New Delhi: ORF and Global Policy Journal, 2024, 189 p.
3. Кваша Т. К. Світові наукові та технологічні тренди у сфері забезпечення національної безпеки [Електронний ресурс] /Тетяна Кваша. К.: УкрІНТЕІ, 2019. 107 с.
4. Писаренко Т.В. Аналіз світових технологічних трендів у військовій сфері: монографія [Електронний ресурс] / Т. Писаренко, Т. Кваша, Т. Гаврис та ін., за заг. редакцією Т.В.Писаренко . К.: УкрІНТЕІ, 2021. 110с.

5G/6G ANTENNA OPTIMIZATION

Pavlos Lazaridis

*Electronic and Electrical Engineering at the University of Huddersfield,
Huddersfield, United Kingdom*

ПОРІВНЯННЯ ЕФЕКТИВНОСТІ ШИРОКОСМУГОВИХ ТА ВУЗЬКОСМУГОВИХ СИГНАЛІВ В УМОВАХ НИЗЬКОЇ ЕНЕРГЕТИКИ

Уривський Л.О., Шмігель Б.О.

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна
E-mail: leonid_uic@ukr.net, bshmigel@gmail.com*

COMPARISON OF THE EFFICIENCY OF BROADBAND AND NARROWBAND SIGNALS IN LOW ENERGY CONDITIONS

In this paper considered a comparative analysis of effectiveness of the communication channel resource of broadband and narrowband signals.

Різні системи зв'язку для передачі дискретних і безперервних повідомлень, незважаючи на їх відмінність як за призначенням, так і за способами реалізації, характеризуються певними кількісними показниками. Основними з них є швидкість і достовірність передачі інформації.

Ефективність використання ресурсів каналу описує показник інформаційної ефективності, який являє собою відношення продуктивності до пропускну здатності каналу зв'язку [1].

Являє інтерес порівняння між собою різні системи зв'язку по мірі ефективності використання ними основних ресурсів каналу — потужності сигналу і займаної смуги частот — і досягнутої при цьому пропускну здатності і продуктивності [2].

На рисунку 1 відображені залежності ефективності використання ресурсів багатопозиційної модуляції і СКК для різних вимог до P_b .

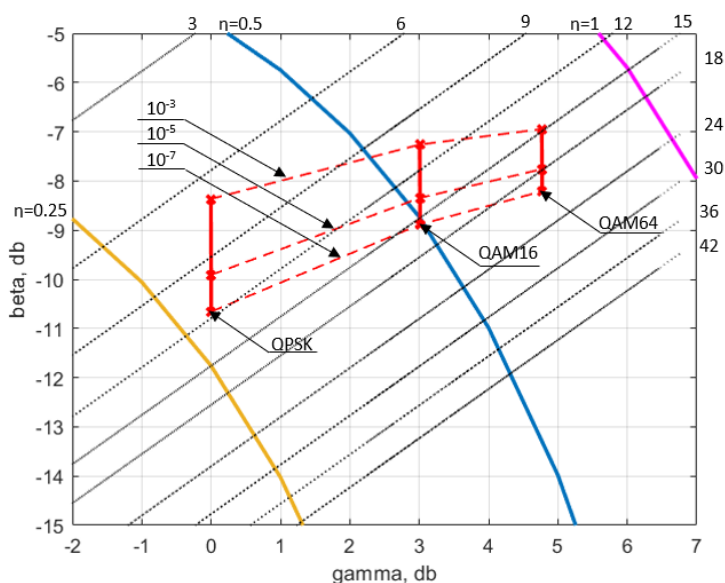


Рис. 1. Показники ефективності використання ресурсів каналів з багатопозиційними сигналами.

Для ширококутового сигналу для забезпечення достовірності 10^{-6} на виході декодера при $V=100$ необхідно забезпечити $h_2 = 19.8$ дБ, при $V=1000$ – $h_2 = 22.4$ дБ, а при $V=10000$ – $h_2 = 27$ дБ. Це пояснюється тим, що потужність завад в смузі частот F при використанні ШСС накопичується в цій смузі в V раз більше шумів в порівнянні зі смугою ВСС.

Використання ШСС змінює підхід до динаміки взаємозалежності частотної та енергетичної ефективності: з зростанням V погіршується інформаційна ефективність η та а енергетична ефективність β , а частотна ефективність γ СПІ залишається незмінною.

Найбільша зміна узагальненої ефективності η має місце при переході від BPSK до ШСС при значенні бази $V=100$ (від значення $\eta = 0,3$ до $\eta = 0,2$).

Яскраво виражена тенденція витрати енергетичного ресурсу для забезпечення більш високої достовірності. В одиницях показника енергетичної ефективності діапазон $-8...-12$ дБ для BPSK при динаміці досяжної достовірності $10^{-3}...10^{-7}$, для $V=100$: $-16,5...-19,5$ дБ, $V=10000$: $-21,5...-23$ дБ.

Разом з тим, новим є наочне відображення тенденції погіршення узагальнених показників інформаційної ефективності при покращенні достовірності сигналів BPSK та ШСС. Можна бачити, що при покращенні достовірності, інформаційний показник η суттєво зменшується на фоні значного погіршення енергетичної ефективності β при практичній стабільності показника частотної ефективності γ .

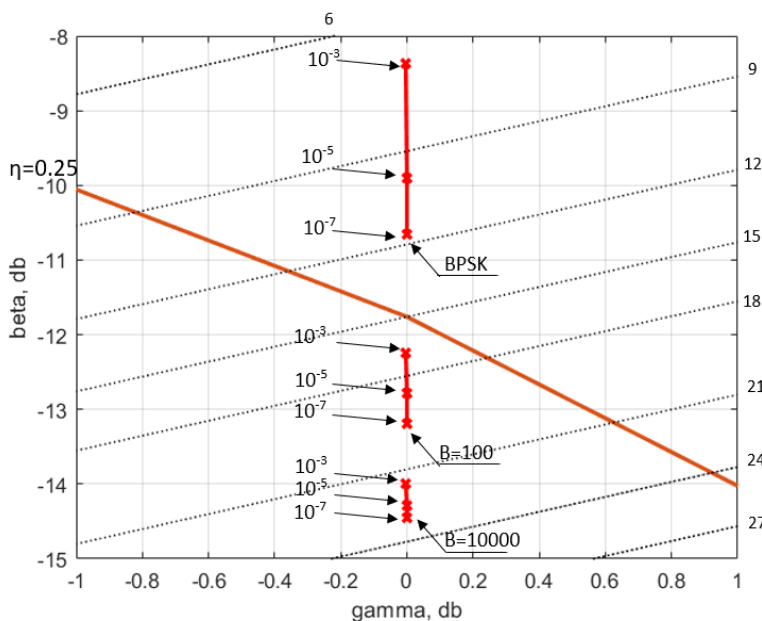


Рис. 2. Показники ефективності використання ресурсів каналів з ШСС та ВСС ФМ з еквівалентною потужністю.

Збільшення позиційності M сигналів QAM- M змінює підхід до динаміки взаємозалежності частотної та енергетичної ефективності: з зростанням M покращується інформаційна ефективність η , частотна ефективність γ СПІ, а також енергетична ефективність β .

Найбільша зміна узагальненої ефективності η має місце при переході від QPSK до QAM-16 (від значення $\eta = 0,3$ до значень $\eta = 0,5...0,6$).

Яскраво виражена тенденція витрати енергетичного ресурсу для забезпечення більш високої достовірності. В одиницях показника енергетичної ефективності діапазон $-8...-11$ дБ для QPSK при динаміці досяжної достовірності $10^{-3}...10^{-7}$, для QAM-16 – це $-7...-8,5$ дБ.

Завдяки додатковій шкалі абсолютних енергетичних ресурсів ($h^2 = Q$) можна оцінити діапазон достовірності для QPSK пов'язаний з енергетичним ресурсом каналу зв'язку $h^2 = 7...15$ дБ, а для QAM-16 – це $h^2 = 15...20$ дБ.

Отже, велика сукупна ефективність сигналів з великим значенням M вимагає більшої потужності сигналу в точці прийому [3].

Застосування нової модифікованої шкали ефективності дозволяє провести комплексну оцінку системи за показниками частотної, енергетичної та узагальненої (інформаційної) ефективності, а також за показником задіяного енергетичного ресурсу h^2 .

При цьому модифікована шкала ефективності дозволяє комплексно оцінити частотну та енергетичну ефективність використання багатопозиційної маніпуляції та завадостійкого кодування. Такий спосіб оцінки розширює спектр пошуку оптимальних за відносним критерієм енергетичної і частотної ефективності систем передачі, а також абсолютним енергетичним показником h^2 , оскільки забезпечує великі можливості варіювання параметрами для досягнення максимальної продуктивності при мінімальних витратах ресурсів каналу зв'язку.

Висновки: Методика дозволяє оцінити ефективність використання ресурсів каналів зв'язку з багатопозиційною маніпуляцією та завадостійким кодуванням, а також кількісно оцінити витрати на реалізацію заходів щодо підвищення достовірності або продуктивності у вимірі запропонованих показників. Такий спосіб оцінки розширює сферу пошуку оптимальних систем передачі, оскільки враховує можливості варіювання параметрами сигналів в каналах зв'язку в широкому діапазоні значень.

Широкосмугові сигнали, не забезпечують кращої достовірності та програють в інформаційній ефективності η та а енергетичній ефективності β , при незмінній частотній ефективності γ . Якщо ШСС має обмеження в ресурсі (обмежена енергія сигналу), то вони ведуть до втрати завадостійкості або розтрати ресурсу, щоб відновити вихідну достовірність. Засобом, що дозволяє підвищити достовірність прийому є завадостійке кодування, однак декодер не може розрізняти спосіб обробки сигналу до його входу, тому при рівній енергетиці і однаковій швидкості символів джерела, ВСС мають перевагу і на цьому етапі обробки сигналів.

Література

1. Уривський Л.О., Шмігель Б.О. Оцінка ефективності використання ресурсів безпроводових каналів зв'язку / Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки. Том 33 (72) № 5 2022. – С. 27-32. – Режим доступу: https://tech.vernadskyjournals.in.ua/journals/2022/5_2022/4.pdf.
2. Основи теорії телекомунікацій / О. В. Корнейко, О. В. Кувшинов, О. П. Лежнюк та ін.; за ред. М. Ю. Ільченка. Київ: ІССЗІ НТУУ «КПІ», 2010. 786 с.
3. Уривський Л.О., Мошинська А.В., Прокопенко К.А. Модифікована методика оцінки ефективності систем передачі інформації. Наукові вісті НТУУ «КПІ». – Київ: 2010. № 6. С. 24-29.

ШТУЧНИЙ ІНТЕЛЕКТ В СФЕРІ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ

Кононова І.В.

*Навчально-науковий інститут телекомунікаційних
систем КПІ імені Ігоря Сікорського, Україна
E-mail: viti21@ukr.net*

ARTIFICIAL INTELLIGENCE IN THE FIELD OF ELECTRONIC COMMUNICATIONS

Information and communication technologies are developing rapidly, changing the way we interact with the technological world. One of the most relevant areas of development of information and communication technologies is artificial intelligence, which has significant potential for transforming industries, improving people's lives, creating new jobs, solving complex problems and stimulating economic growth.

The material was prepared for students, teachers and engineers based on the news digest of the Educational and Research Institute of Telecommunication Systems.

Навчально-науковий інститут телекомунікаційних систем КПІ імені Ігоря Сікорського активно інформує студентів та викладачів про новини в сфері електронних комунікацій через телеграм канал Деканат та сайт інституту. Це допомагає студентам та всім зацікавленим особам бути в курсі останніх тенденцій, подій і розвитку цієї важливої галузі. Такий підхід сприяє збагаченню знань студентів та підвищенню загальної обізнаності.

За період створення новин інфотелекому було опубліковано: 1852 новини. В 2020 році – 333 новини, у 2021 році – 486 новин, у 2022 році – 459 новин; у 2023 році – 428 новин, а з початку 2024 року – 146 новин.

Останній час тема штучного інтелекту (ШІ) стала дуже актуальною в сучасному світі завдяки стрімкому розвитку ІТ-сфери, появі нових передових технологій та прагненню вдосконалювати, модернізувати та автоматизувати сучасне життя.

Поняття штучного інтелекту виникло ще в середині ХХ століття, і з тих пір ідея розвитку систем, здатних до самонавчання, прийняття рішень та виконання завдань, вже була предметом досліджень інженерів та науковців. Протягом останніх десятиліть штучний інтелект переживав періоди піднесення та спаду за інтересом, але саме в останні роки він став особливо актуальним завдяки поєднанню передових обчислювальних можливостей, розвитку алгоритмів машинного навчання та нейронних мереж, а також доступності великого обсягу даних для аналізу. Термін "штучний інтелект" був введений Дж. Маккарті, який є лауреатом премії Тьюрінга за свій внесок у дослідження в галузі ШІ. Він визначив ШІ як "спосіб зробити комп'ютер або програму, здатну мислити так само розумно, як людина". Наприклад, вчені в галузі теорії обчислень, такі як Барр та Файгенбаум, розглядають ШІ як галузь інформатики, що займається розробкою інтелектуальних комп'ютерних систем, які мають можливості, традиційно пов'язані з

людським розумом - розуміння мови, навчання, здатність мислити та розв'язувати проблеми та інше.

Інтерес до штучного інтелекту зростає з кожним днем, і це стає помітним явищем у всьому світі. Передові країни вкладають величезні ресурси в дослідження та розробки в галузі штучного інтелекту, змагаючись між собою в нових інноваціях та проєктах, зосереджуючись на розробці нових технологій, які можуть застосовуватися в різних галузях, таких як медицина, транспорт, освіта, машинобудування, робототехніка та багато інших. Зростання інтересу свідчить про впевненість у тому, що ШІ може стати ключовим каталізатором для розвитку суспільства та економіки, забезпечуючи нові можливості, підвищену ефективність та конкурентоспроможність. Розширення досліджень і впровадження інноваційних рішень у галузі штучного інтелекту відкриває широкі перспективи для майбутнього і може принести значні соціальні та економічні вигоди.

На сьогоднішній день існують три основні цілі розвитку штучного інтелекту:

Автоматизація і оптимізація людської праці: Першою і, можливо, найголовнішою ціллю є заміщення і оптимізація трудових процесів людини за допомогою штучного інтелекту. Компанії та розробники працюють над створенням інтелектуальних систем, які можуть автоматизувати та покращувати продуктивність праці.

Створення комп'ютерних моделей для імітації процесів розв'язання складних завдань: Другою ціллю є розробка комп'ютерних моделей, які можуть імітувати процеси розв'язання інтелектуальних завдань. Це допомагає краще зрозуміти природу самого процесу та витягнути максимум для подальшого розвитку та побудови інтелектуальних систем.

Створення підсилювача інтелекту: Третя ціль стала результатом двох попередніх. Ідеальний план розвитку штучного інтелекту передбачає, що він перевершить природний інтелект людини, або принаймні стане його рівнем. Це має призвести до посилення інтелекту людини завдяки синергії між ним і штучним інтелектом.

В усьому світі науковцям вдалося створити значний фундаментальний базис у галузі штучного інтелекту, розробивши методи, які включають: машинне навчання для обробки зображень та розпізнавання образів; автономна координація та управління; колективна взаємодія роботів для вирішення групових завдань; когнітивні комп'ютерні моделі з розумінням природної мови; системи підтримки наукових досліджень; а також автоматизація мислення, планування та управління поведінкою.

Дослідження та розробка ШІ стало ключовим напрямком для багатьох великих технологічних компаній:

Google: Google володіє великими знаннями в галузі машинного навчання та глибокого навчання. Вони розробляють рішення для розпізнавання мови, обробки природної мови, комп'ютерного зору, рекомендаційних систем, автономного водіння та інших областей.

Facebook: Facebook активно застосовує штучний інтелект для впровадження систем рекомендацій, фільтрації новин, розпізнавання обличчя та автоматичного перекладу мови.

Amazon: Amazon використовує ШІ для вдосконалення процесів електронної комерції, таких як персоналізовані рекомендації, прогнозування попиту, автоматизоване управління запасами та чат-боти для обслуговування клієнтів.

Microsoft: Microsoft веде дослідження в галузі машинного навчання, розробляючи рішення для різних сфер, включаючи обробку мови, комп'ютерний зір, медицину, фінанси та інші.

IBM: IBM спеціалізується на розробці систем штучного інтелекту для підприємств, таких як системи аналізу даних, прогнозування витрат, управління ланцюгами постачання та інші.

Tesla: Tesla розробляє системи автопілоту та автономного водіння, які базуються на штучному інтелекті та глибокому навчанні для аналізу дорожньої ситуації та прийняття рішень.

OpenAI: OpenAI займається дослідженнями у галузі штучного інтелекту та розробляє різноманітні моделі глибокого навчання та машинного навчання для різних застосувань, включаючи генерацію тексту, комп'ютерний зір та ігрові системи.

General Electric (GE): Використання ШІ для розробки автономних роботів дозволяє компанії GE автоматизувати складні завдання, такі як сборка та монтаж, що раніше виконували люди. Це допомагає підвищити продуктивність та уникнути помилок.

Siemens: Використання ШІ для розробки систем аналізу даних дозволяє Siemens відслідковувати ефективність виробничих ліній і виявляти потенційні проблеми заздалегідь. Це допомагає у покращенні якості продукції та уникненні відходів.

Toyota: Використання інструментів ШІ в системах «штучного зору» дозволяє Toyota контролювати якість деталей, виготовлюваних на виробничих лініях. Це сприяє підвищенню якості та ефективності виробництва.

Ці компанії витрачають значні кошти на розробку нових технологій, алгоритмів та продуктів ШІ з метою поліпшення своїх послуг, створення нових продуктів та вирішення складних завдань.

За даними агентства Deep Knowledge Analytics, Україна входить до трійки країн Східної Європи за кількістю ІТ-компаній, що працюють у сфері штучного інтелекту. Розглянемо декілька проєктів, які вже досягли успіхів у цій галузі:

Preply: онлайн-платформа для навчання іноземних мов з використанням індивідуальних уроків з викладачами з усього світу. Штучний інтелект використовується для підбору найкращих викладачів для кожного студента, а також для адаптації навчальних матеріалів до потреб кожного користувача.

People.ai: компанія розробляє інструменти для автоматизації процесів управління взаємодією з клієнтами, використовуючи аналіз даних та

штучний інтелект. Їх платформа допомагає компаніям ефективніше взаємодіяти з клієнтами та збільшувати продажі.

GitLab: компанія розробляє систему управління версіями ісходних кодів, яка використовує штучний інтелект для автоматизації процесів розробки програмного забезпечення та управління проектами.

Lookery: компанія створила технологію розпізнавання обличчя для відеозв'язку, яка використовує штучний інтелект для покращення якості та реалістичності обміну зображеннями.

Grammarly: Grammarly є однією з найвідоміших українських технологічних компаній, яка розробляє програми для перевірки правопису та граматики. Вони використовують штучний інтелект для постійного вдосконалення своїх алгоритмів та розробки нових функцій.

Reface: розробляє додаток для обміну обличчя здобув значний успіх, особливо завдяки своїй технології глибокого навчання, яка дозволяє реалістично переносити обличчя користувачів на фотографії та відео.

Отже, сучасний етап розвитку суспільства характеризується підвищенням темпів інноваційного прогресу, а системи штучного інтелекту є його основними динамічними силами. Розробка та впровадження штучного інтелекту переходить на новий рівень свого розвитку. Все частіше звучить твердження про наближення нової ери кіборгізації, а також гібридизації - наступного кроку в розвитку інтелектуальної робототехніки різного призначення. Спостерігається тенденція стрімкого розвитку науково-технологічних розробок у галузі штучного інтелекту та прискорення їх практичного використання.

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

Література

1. <https://forbes.ua/innovations>
2. <https://gwamedia.com/tendenczii-rozvitku-shtuchnogo-intelektu-v-ukraini-ta-sviti/>
3. <https://dou.ua/forums/topic/38312/>
4. <https://expert.com.ua/>
5. <https://www.ukrinform.ua/>
6. <https://internetua.com/>
7. <https://www.ukrinform.ua/>
8. <https://tech.liga.net/>
9. <https://prostomob.com/>
10. <https://processer.media/>

**SCIENTIFIC AND PRACTICAL ACTIVITIES
STUDENTS OF THE ER ITS**

Kostiantyn Lisovskyi

*Educational and Scientific Institute of Telecommunication
Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine*

Секція 1. Достовірність та ефективність передачі інформації

УДК 621.382

МЕТОД АДАПТИВНОГО УПРАВЛІННЯ ПРОЦЕСОМ ДЕКОДУВАННЯ ТУРБОПОДІБНИХ КОДІВ

Лівенцев С.П., Созонник Г.Д.

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна
E-mail: slivencev@gmail.com*

A METHOD FOR ADAPTIVE CONTROL OF THE PROCESS OF DECODING TURBO-LIKE CODES

A method for obtaining a parity check code based on the decomposition of an information sequence into an n -dimensional array, combining ease of implementation and high reliability, has been developed; a perforated modification of this code has been proposed, taking into account the specifics of errors that occur when decoding turbocodes (TC) and providing greater reliability and less redundancy in the field of signal-to-noise ratio (SNR) with a predominance of decoded packets..

Важливою особливістю турбоподібних кодів (ТК) є те, що вони належать до кодів, що виправляють помилки, і використовують ітеративне декодування. З цього випливає, що після корекції канальної послідовності на певній ітерації декодер повинен класифікувати отриману інформаційну послідовність як задовільну або помилкову.

Висока обчислювальна складність процесу декодування ТК передбачає оптимізацію роботи декодера. Одним з можливих рішень цього завдання є відмова від процедури декодування з фіксованою кількістю ітерацій та застосування алгоритмів управління турбодекодером, що дозволяють скорочувати кількість ітерацій, що виконуються. Для підвищення достовірності пакета, що декодується, частина інформаційної послідовності ТК використовується для передачі перевірючих біт вкладеного завадостійкого коду [1].

Передача даних у системах із ТК є пакетною. Пакет є звичайною послідовністю інформаційних біт без заголовку. Протягом сеансу роботи декодер обробляє множину пакетів, кожен біт в яких зазнав канальних спотворень. Позначимо множину пакетів a_k , що передаються як M , а підмножини коректних та некоректних переданих (оброблених) пакетів – як T і F ($T \cup F = M$). Завдання алгоритму управління процесом турбодекодування полягає у прийнятті рішення про те, до якої підмножини належить пакет a_k . Це досягається з використанням пари правил класифікації $f(a_k)$ і $g(a_k)$, кожне з яких є предикатом і повертає істину, якщо пакет визнаний коректним.

Суть першого правила $f(a_k)$ полягає у перевірці вкладеного в інформаційну послідовність ТК коду, що реєструє помилки. Така методика є специфічним випадком каскадного кодування. Справа в тому, що ТК як код, що виправляє помилки, здійснює корекцію інформаційних біт, проте сам по собі не може реєструвати помилки. Зовнішній код перевірки парності належить до кодів, що реєструють помилки, тобто. неспроможний здійснювати корекцію. Запропонований метод заснований на спільному використанні подібної пари кодів

з функціональністю, що не перетинається [2].

Після закінчення ітерації турбодекодування, інформаційна послідовність ТК a_k міститиме виправлені інформаційні біти $q(a_k)$ та перевірочні біти вкладки коду $p(a_k)$. Якщо за допомогою послідовності виправлених інформаційних біт $q(a_k)$ з використанням відомого алгоритму кодування E вдається отримати послідовність виправлених перевірочних біт $p(a_k)$, можна говорити, що інформаційна послідовність ТК була декодована коректно. Формальний запис подібного правила матиме вигляд:

$$\begin{aligned} f(a_k) &= 1, \text{ при } E(q(a_k)) = p(a_k) \\ f(a_k) &= 0, \text{ при } E(q(a_k)) \neq p(a_k). \end{aligned} \quad (1)$$

Суть другого правила g полягає у перевірці правила зупинки турбодекодера. Найбільш очевидним правилом зупинки декодера ТК є порівняння "жорстких" рішень, вироблених декодером на одній або кількох послідовних ітераціях (Н-метод).

Подібні методи розглядаються у [3]. Нехай система, що обробляє K інформаційних біт, на $n \leq N_{max}$ ітерації, яка для кожного i біта ($1 \leq i \leq K$) використовує "жорсткі" рішення двох декодерів $u_{i,1}^n$ і $u_{i,2}^n$ для поточної ітерації. Використання інформації про "жорсткі" рішення з попередніх ітерацій знижуватиме достовірність через те, що з кожної ітерації декодер здійснює корекцію інформаційних біт, тобто. попередні ітерації будуть містити значення з дедалі більшою недостовірністю. Формальний запис правила зупинки матиме такий вигляд:

$$\begin{aligned} g(a_k) &= 1, \text{ при } \forall i, 1 \leq i \leq K, u_{i,1}^n = u_{i,2}^n \\ g(a_k) &= 0, \text{ при } \exists i, 1 \leq i \leq K, u_{i,1}^n \neq u_{i,2}^n. \end{aligned} \quad (2)$$

З урахуванням двох описаних вище предикатів $f(a_k)$ і $g(a_k)$, пакет a_k належатиме достовірній підмножині, якщо

$$a_k \in (T | f(a_k) = 1 \vee g(a_k) = 1). \quad (3)$$

Далі розглядається випадок управління турбодекодером, у якому правило зупинки $g(a_k)$ залишається незмінним, а вкладений код, який реєструє помилки $f(a_k)$ може змінюватися. Необхідно знайти такий вкладений код, при використанні якого потужність множини T буде максимальною. У формальному вигляді завдання може бути сформульовано як

$$\begin{cases} g = const \\ \max_f |T| \end{cases} \quad (4)$$

Розглянемо роботу типової системи передачі з ТК, кодер якої використовує два паралельно з'єднаних компонентних кодера: рекурсивних згорткових кодерів (РЗК) розділених перемежувачем [4]. Довжина кодової послідовності (пакета), що передається каналом, збігається з обсягом перемежувача. Як метод перемежування використовується псевдовипадкова перестановка. Компонентний РЗК ініціалізується за допомогою поліноміального генератора $G = (5/7)$, як найпростішого. Швидкість кодування становить $1/3$ (перфорація не застосовується). Гранична кількість ітерацій N_{max} вибрано рівним восьми. Як алгоритм декодування для компонентного декодера обраний $MAX-LOG-MAP$ (наближений, по відношенню до MAP) як найпростіший з точки зору обчислювальної складності. Структура кодера та декодера ТК детально описана у [5].

При моделюванні роботи системи передачі використовувався канал з адитивним білим гаусівським шумом, Відношення сигнал-шум (ВСШ) змінювалося від 0 до 4 дБ: надалі – робоча область. При виконанні імітаційного моделювання ВСШ змінювалося з кроком 0,2 дБ.

Результати моделювання роботи системи передачі з ТК, що використовує різні способи управління декодером, показано на рис. 1.

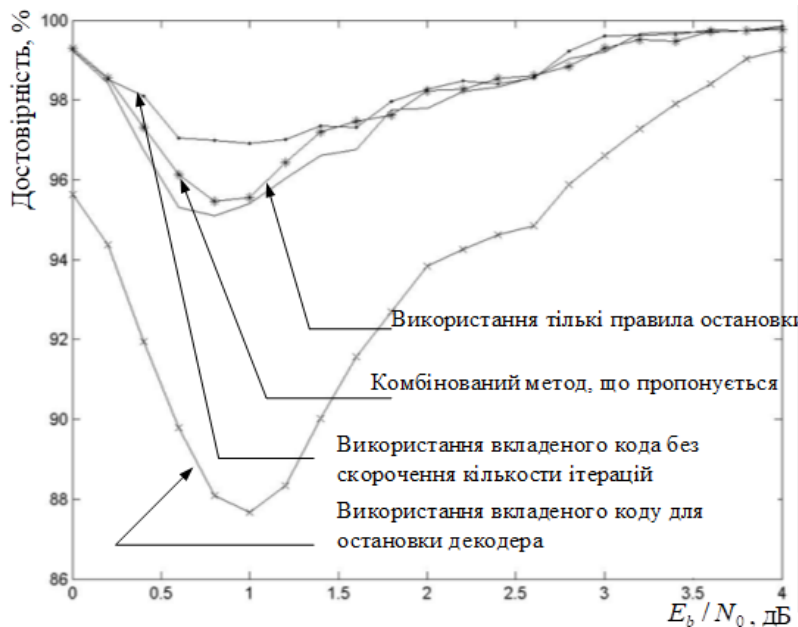


Рис. 1. Залежність достовірності декодованого пакета від ВСШ при використанні різних методик зупинки турбодекодера.

Як бачимо, окреме використання вкладки коду перевірки парності для керування роботою турбодекодера пов'язане з декодуванням пакетів з низькою достовірністю. З іншого боку, будь-який метод, пов'язаний зі скороченням кількості виконуваних ітерацій, буде викликати зниження достовірності пакета, що декодується в порівнянні з фіксованою кількістю ітерацій. Застосування правил зупинки управління роботою ТК показує кращу достовірність, ніж використання вкладки коду,

проте спільне використання цих методів оптимально.

Значна відмінність реальної кількості ітерацій від ідеальної в нижній частині робочої області пов'язана з тим, що всі методи управління, що розглядаються, можуть достроково зупинити процес декодування тільки в тому випадку, якщо цей пакет може бути декодований коректно, а в нижній ділянці робочої області переважають недекодовані пакети.

Пропонується новий метод формування коду, що реєструє помилки, який заснований на розкладанні інформаційної послідовності ТК в n -мірний масив. Тоді кожен інформаційний біт n раз братиме участь у формуванні біт контрольної суми. На рис. 2 показаний приклад розкладання 25 бітної послідовності при $n = 2$ і 64 бітної при $n = 3$.

У першому випадку інформаційний біт $X1$ бере участь у формуванні біт $A1$ і $B1$ контрольної суми, а у другому – біт $X2$ буде впливати на $A2$, $B2$ і $C2$.

Розглянемо обернену задачу: розкладання n -мірного масиву в одновірний. Нехай індексація елементів n -мірного масиву виконується таким чином: $a(idx_1, idx_2, \dots, idx_n)$. Нехай i -й індекс змінюється в діапазоні від 0 до $m - 1$ ($0 \leq idx_i < m$).

Для зручності припустимо, що максимальне значення індексу з кожної розмірності дорівнює m . Таким чином масив є n -мірний гіперкуб.

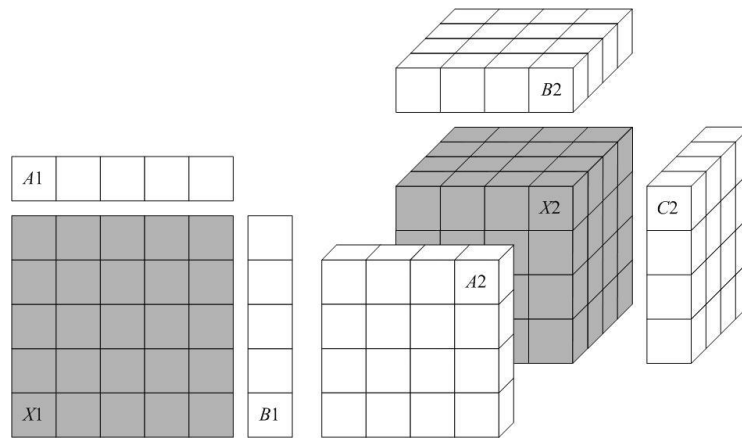


Рис. 2. Подання бітової послідовності дво- та тривимірним масивом.

Нехай останній, n -й індекс багатовимірного масиву є наймолодшим, тоді елемент $a(idx_1, idx_2, \dots, idx_n)$ n -мірного гіперкуба при розкладанні в одновимірний масив матиме індекс:

$$idx = idx_n + idx_{n-1} \cdot m + idx_{n-2} \cdot m^2 + \dots + idx_1 \cdot m^{n-1}. \quad (5)$$

Отримання біт контрольної суми в загальному випадку для n розмірностей здійснюватиметься таким чином:

1. Для обраної i -ї розмірності отримуємо множину індексних наборів $(idx_1, idx_2, \dots, idx_i, \dots, idx_n)$ таких, що всі інші індекси, крім i -го приймають усі можливі комбінації значень. Усього така множина міститиме m^{n-1} елементів.

2. Кожному елементу цієї множини буде відповідати один перевірочний біт. Для його отримання слід підсумувати (за модулем 2) інформаційні біти, що отримані змінною i -го індексу

$$p = \sum_{idx_i=0}^{m-1} a(idx_1, idx_2, \dots, idx_i, \dots, idx_n) \quad (6)$$

3. Дію 2 необхідно повторити для кожного індексного набору.

4. Дію 1 необхідно повторити для кожної розмірності.

При використанні такого методу отримання біт контрольної суми результуюча послідовність міститиме $m^n + n \cdot m^{n-1}$ біт, де перший доданок відповідає за кількість інформаційних біт, другий – за кількість перевірочних біт.

Як показано на рис. 3 використання запропонованого модифікованого коду перевірки парності призводить до збільшення достовірності декодованого пакета порівняно з класичним випадком.

З рис.3 видно, що у найбільш проблемній ділянці робочої області значення достовірності для звичайного коду перевірки парності становить 98,43%, а модифікованого коду – 99,87% при тому, що звичайний код має більшу надмірність.

Недоліком запропонованого методу отримання коду перевірки парності є те, що зі збільшенням параметра n частка перевірочних символів збільшуватиметься. Можна відзначити, що з різних значення ВСШ зі збільшенням рівня завад інформаційна послідовність ТК для оптимального випадку вимагатиме більшої кількості перевірочних біт, і з зменшенням – меншої. Вже при ВСШ в 2 дБ потреба у вкладеному коді фактично відпадає і для всієї інформаційної послідовності достатньо одного перевірочного біта.

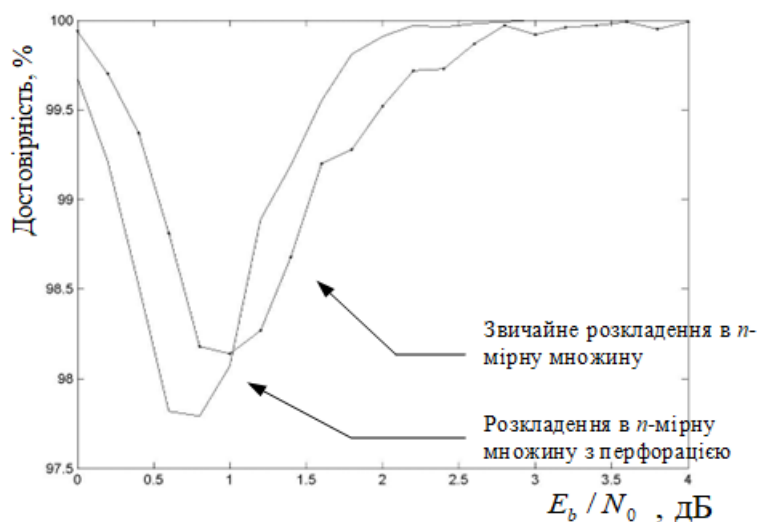


Рис. 3. Порівняння достовірностей декодованих пакетів при використанні звичайного та модифікованого кодів перевірки парності.

Аналогічну задачу знаходження оптимальної кількості перевірючих біт можна вирішувати і для запропонованого коду перевірки парності, що використовує розкладання інформаційної послідовності в n -мірний масив. У цьому випадку необхідно буде визначити оптимальний спосіб перфорації перевірючих біт (фактично оптимальну швидкість коду перевірки парності), при якому система демонструватиме максимальну ефективність.

Таблиця 1. Оптимальні довжини коду перевірки парності при змінному ВСШ.

E_b/N_0	0,5 дБ	1 дБ	1,5 дБ	2 дБ
Оптимальний код перевірки парності (n, k)	(49,50)	(79,80)	(199,200)	(399,400)

Наявність подібної залежності дозволить проектувати систему передачі інформації з ТК, що використовує вкладений адаптивний код, що реєструє помилки та підвищує достовірність переданого пакета

Розроблено метод отримання коду перевірки парності, заснований на розкладанні інформаційної послідовності в n -мірний масив, що поєднує простоту реалізації та високу достовірність; запропонована перфорована модифікація даного коду, що враховує специфіку помилок, що виникають при декодуванні ТК і забезпечує більшу достовірність і меншу надмірність в області ВСШ з переважанням пакетів, що декодуються. Розглянуто завдання пошуку коду перевірки парності з оптимальною надмірністю для реєстрації помилок інформаційної послідовності ТК.

Література

1. Berrou C., Glavieux A., P. Thitimajshima Near Shannon limit error-correcting coding and decoding: turbo-codes // in Proc. Int. Conf. On Commun., ICC-93. – 1993. – Geneva. – Switzerland. – May. – P. 1064-1070.
2. Consultative Committee for Space Data Systems, Telemetry Channel Coding. Blue Book, vol. 101.0-B-4, issue 4, May 1999. <http://www.ccsds.org/documents/pdf/CCSDS-101.0-B-4.pdf>.
3. A. Matache, S. Dolinar, F. Pollara Stopping Rules for Turbo Decoders // TMO Progress Report 42-142. - Jet Propulsion Laboratory, California Institute of Technology. - August 15, 2000.
4. Р. Морелос-Сарагоса. Мистецтво завадостійкого кодування. Методи, алгоритми, застосування. Переклад з англійської В.Б. Афанасьєва ТЕХНОСФЕРА.- М.-2005 - 320 с.
5. С.В.Зайцев, С.П.Лівенцев, Б.В.Горлинський, А.І.Артюх. Імітаційне моделювання характеристик завадостійкості системи передачі інформації з турбокодами // Зв'язок. - 2006. - №7. - С. 38-42.

ОЦІНКА ШВИДКОСНИХ ХАРАКТЕРИСТИК ТЕХНОЛОГІЇ VDSL2-VECTORING В УМОВАХ ПЕРЕХІДНИХ ЗАВАД

Носков В.І.

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

ESTIMATION OF SPEED CHARACTERISTICS FOR VDSL2-VECTORING TECHNOLOGY UNDER CROSS TALKING INTERFERENCE CONDITION

VDSL2-vectoring technology is an improvement of the widely known VDSL2 technology, which is used as the "last inch" for fiber optic broadband access networks in FTTC (Fiber To The Curb/Cab) and FTTB (Fiber To The Building) architectures to provide a variety of multimedia services, including IPTV, OTT and others. VDSL2-vectoring technology allows you to compensate a cross talking interference at the far end of the cable (FEXT) and, thus, significantly increase the transmission speed in the section from the access point to the customer premises. Since FEXT depends on the cable length, it is interesting to determine the range of distances at which it is appropriate to use VDSL2-vectoring technology.

Технологія VDSL2-vectoring є вдосконаленням поширеної технології VDSL2, яка використовується у якості «останнього дюйму» в оптоволоконних широкосмгових мережах доступу в архітектурі FTTC (Fiber To The Curb/Cab) та FTTB (Fiber To The Building) для надання різноманітних мультимедійних послуг, включаючи IPTV, OTT та інших. Технологія VDSL2-vectoring дозволяє компенсувати вплив перехідних завад на дальньому кінці кабелю (FEXT) і, таким чином, значно збільшити швидкість передачі на ділянці від точки доступу до приміщень користувачів. Так як FEXT залежить від довжини кабелю, то цікавим є визначення діапазону відстаней, на яких доцільно використовувати технологію VDSL2-vectoring.

Технологія VDSL2 (ITU-T G.993.2) є високошвидкісною технологією, що використовується на останній ділянці оптоволоконної мережі доступу, довжина якої не перевищує 1 км.

Технологія VDSL2 працює по мідному кабелю, використовує лінійний сигнал DMT (Discrete Multi Tone) з кількістю несучих до 8192 (профілі 35a та 35b) і кроком несучих у 4,3125 кГц. Частотні канали, утворені за рахунок QAM-модуляції несучих, поділяються на дві групи, які використовуються у напрямках Downstream (від DSLAM до користувачів) та Upstream (у зворотному напрямку). Таким чином, смуги частот передачі і прийому не пересікаються і при організації багатьох ліній VDSL2 у спільному кабелі між ними мають місце тільки перехідні завади на дальньому кінці кабелю, які визначаються коефіцієнтом перехідних завад FEXT (Far End Cross Talking). Перехідні завади на дальньому кінці кабелю залежать від його довжини та частоти сигналу. Для оцінки впливу перехідних завад на дальньому кінці кабелю використовують таке поняття як захищеність на дальньому кінці кабелю, яке є відношенням потужності сигналу до потужності перехідної

завади на дальньому кінці кабелю і позначається як ELFEXT (Equal Level FEXT). Для оцінки ELFEXT в поширеному на мережах кабелю типу ТПП пучкової скрутки існує наступна емпірична формула [3]:

$$ELFEXT(f, l, m) = 56 - 6 \lg(m - 1) - 20 \lg\left(\frac{f}{300}\right) + 10 \lg\left(\frac{l}{280}\right), \quad (1)$$

де: f – частота, кГц; l – довжина кабелю, м; m – кількість пар, що використовуються в кабелі для організації VDSL2-ліній; 56 дБ – відповідає мінімально допустимому значенню захищеності на дальньому кінці лише для двох взаємо-впливаючих пар в елементарному пучку кабелю завдовжки 1 км на частоті 300 кГц; 280 – довжина кабелю в метрах, для якої були визначені компоненти формули.

Перехідна завада на дальньому кінці кабелю є адитивною до сигналу DMT. В результаті DMT-символи в точці прийому змінюють амплітуду і фазу. Це проявляється у відхиленні координат сигнальної точки прийнятого символу від того, що очікується (рис. 1).

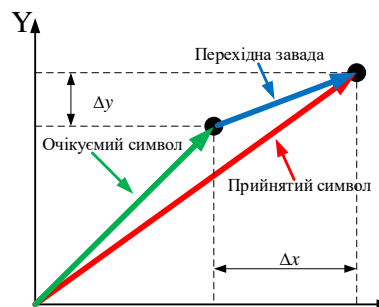


Рис. 1. Результат впливу перехідної завади на прийом символів.

Відхилення вектору символу призводить до помилки в прийнятті рішення про поточний символ. Для компенсації впливу перехідних завод на дальньому кінці кабелю була запропонована технологія «векторингу» (ITU-T G.993.5) як вдосконалення стандарту VDSL2. Технологія «векторингу» використовує корекцію амплітуди та фази символів DMT так, щоб на приймальній стороні після впливу перехідних завод їх амплітуда та фаза відповідали правильним значенням (рис. 2).

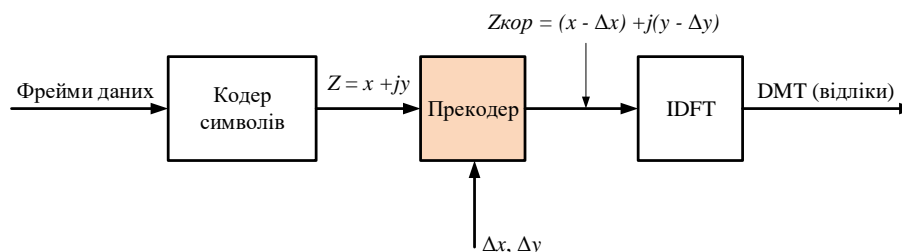


Рис 2унок. Коригування координат сигнальних точок при «векторингу».

Функціональний вузол керування «векторингом» в модемі користувача вираховує відхилення по двом координатам сигнальної точки (Δx та Δy) для символів пілотних послідовностей і надсилає повідомлення в DSLAM.

Прийнявши це повідомлення, DSLAM в спеціальному прекодері віднімає від координат сформованих сигнальних точок значення відхилень, тобто корегує їх положення. Треба зауважити, що сигнали передачі повідомлень про відхилення координат сигнальних точок самі по собі створюють перехідні завади. Таким чином, повністю компенсувати перехідні завади неможливо. Для оцінки ступеню компенсації FEXT вводиться коефіцієнт компенсації (K_{FEXT}) [3], який визначається відношенням потужності перехідних завад в будь-якій парі без застосування «векторингу» до потужності перехідних завад з використанням «векторингу». Як зазначено в [3], цей коефіцієнт при умові однакової потужності передавачів (практично завжди виконується), $m \geq 2$ та однаковому значенні FEXT між будь-якими парами можна записати наступним чином:

$$K_{FEXT}(\text{дБ}) = ELFEXT(m, f, l) - 10\lg(m - 1) \quad (2)$$

За допомогою програми xDSLcalc розраховані залежності швидкості передачі в кабелі ТПП 20x2x0,4 пучкової скрутки від довжини кабелю як без «векторингу», так і з «векторингом», враховуючи, що ELFEXT для такого кабелю на частоті 1000 кГц та довжині 1 км становить орієнтовно 41 дБ [3]. Результати розрахунків залежності швидкості передачі від відстані з використанням векторингу та без нього наведені на рис. 3.

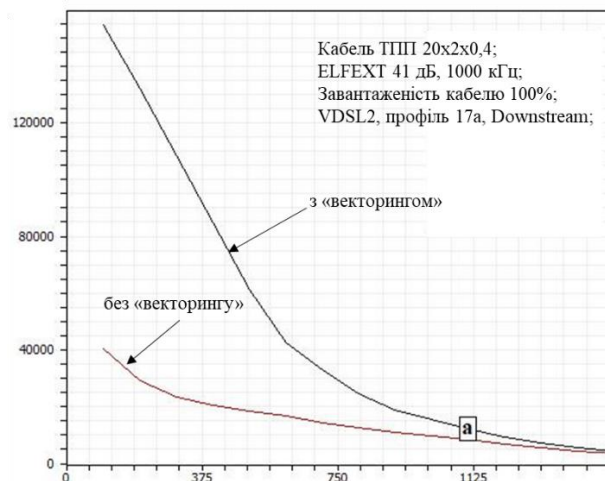


Рис. 3. Залежності швидкості передачі від відстані з використанням «векторингу» та без.

З отриманих результатів (рис. 3) слідує, що технологія VDSL2 vectoring суттєво збільшує швидкість передачі навіть при 100% завантаженні кабелю на відстанях до 1 км. На більших відстанях, внаслідок зниження рівня перехідних завад на дальньому кінці кабелю, використання VDSL2 vectoring практично не дає ніякого ефекту в плані збільшення перепускної здатності лінії VDSL2.

Література

1. ITU-T Recommendation G.993.2, 2019
2. ITU-T Recommendation G.993.5, 2019
3. Balashov V.O., Lyakhovetskiy L.M., Oreshkov V.I. "Broadband access features by VDSL2 technology using crosstalk compensation system «vectoring»." SWorld Scientific Issue №3 (2015). Volume 3: 186-193.

ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ DWDM OVER CWDM В ОПТИЧНИХ МЕРЕЖАХ ДОСТУПУ

Ліла Д.В., Бердников О.М.

*Інститут спеціального зв'язку та захисту інформації, КПІ ім. Ігоря Сікорського, Україна
E-mail: dimalila61@gmail.com; 2507bot@gmail.com*

APPLICATION OF DWDM OVER CWDM TECHNOLOGY IN OPTICAL ACCESS NETWORKS

Implementation of the combined DWDM over CWDM technology on optical access networks provides an opportunity to increase the bandwidth of such networks by increasing the number of optical paths formed. When “AWG” technology is used for optical multiplexing, their number increases up to 10 times, and the implementation of “AWG” technology for optical multiplexing together with the “Interleaving” procedure provides an increase of up to 20 times.

Впровадження ВОСП за технологією спектрального ущільнення (СУ) *CWDM (Coarse Wavelength Division Multiplexing)* в оптичні мережі доступу (ОМД) здійснюються наростаючими темпами. Це викликано виходом корпоративних абонентів за межі міської розподільної мережі і значним зростанням пропускної здатності корпоративних ОМД, що продовжують трансформувати шляхи спільного використання в ОМД технології *CWDM* та інших технологій СУ: *WDM, DWDM, HDWDM* тощо. Практично сьогодні в ОМД відбувається інтегрування технологій *CWDM* та *DWDM* в єдину *DWDM over CWDM* з подальшим їх розвитком для створення гібридних мереж, які об'єднують магістральні, розподільні і місцеві оптичні мережі в єдину оптичну транспортну мережу.

Один з варіантів застосування ВОСП *CWDM* в ОМД (направлення приймання) пояснює рис. 1, який надає варіант перетворення 10 оптичних потоків технології *SDH* рівня *STM-16* (2,5 Гбіт/с) в 10240 потоків *E1* і як ці потоки відеоімпульсів поступають у двадцять 512-квартирних будівель для обслуговування 10240 абонентів (аб). З центрального оптичного вузла зв'язку (ЦОВ) 10 потоків рівня *STM-16*, що прийняті з виходу оптичного демультимплектора *ODMX (Optical Demultiplexer)* фотонного лінійного терміналу *PLT (Photon Transport Terminal)* магістральної ВОСП *CWDM*, потрібно передати на оптичне мережне закінчення ОМД. Для цього, при двосторонньому обміні, необхідно використовувати 10 пар ОВ. Але якщо на ЦОВ встановлюється ВОСП *CWDM* з оптичним мультиплексором *OMX (Optical Multiplexer)* технології *AWG-10 (Arrayed Waveguide Gratings – дифракційна фазова решітка на масиві хвилеводів)*, на десять входів якого подаються зазначені 10 потоків, тоді для передачі такого навантаження достатньо однієї пари волокон. На виході *OMX* утворюється оптичний потік зі швидкістю передачі 25 Гбіт/с. Цей потік вводиться в волокно і передається до місця розташування оптичного мережного терміналу *ONT (Optical Networks Terminal)*, наприклад, в технічне приміщення одного з

обслуговуваних будинків рис. 1. Тут прийнятий потік демультимплексується на 10 оптичних потоків рівня *STM-16*, кожен з яких далі роз'єднується на 16 потоків рівня *STM-1*. В результаті в пункті установки обладнання *ONT* приймається $10 \times 16 = 160$ потоків рівня *STM-1*. Ці потоки поступають на 160 оптичних приймачів де й закінчується *ONT*. Отримані на виході приймачів 160 потоків відеоімпульсів в електронному демультимплексорі–*DMUX* перетворюються в $160 \times 64 = 10240$ потоків *E1*, які розводяться по квартирах (аб).

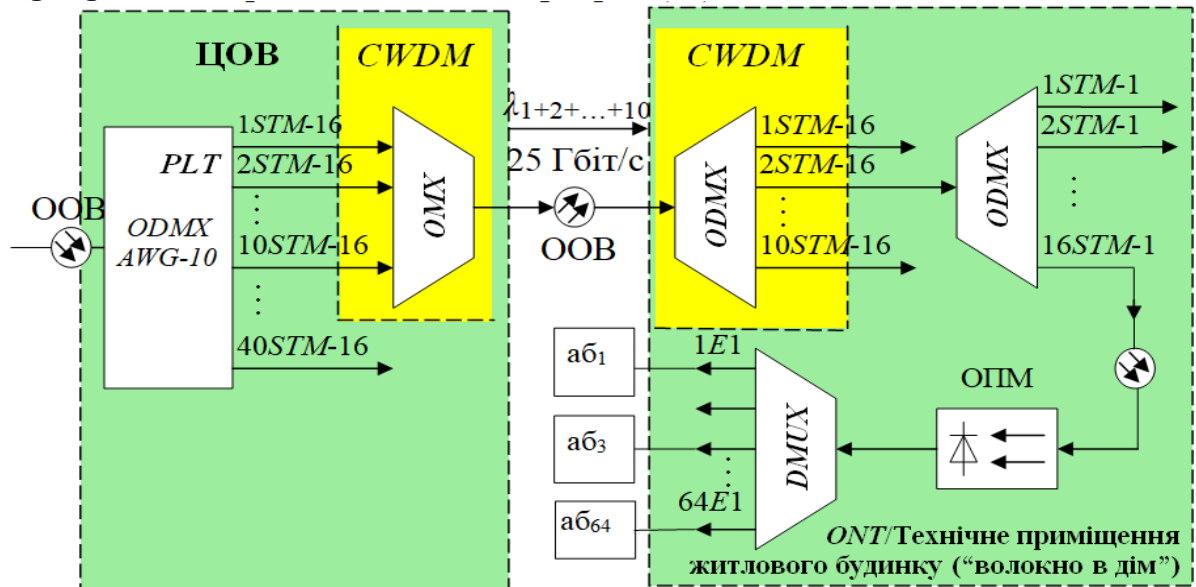


Рис. 1. Варіант застосування ВОСП CWDM в ОМД (направлення приймання).

Практично це формується для мікрорайону міста де знаходиться шістнадцять 16-поверхових 512-квартирних будинків на 8 під'їздів. У під'їзді на майданчику кожного поверху 4 квартири. В результаті в під'їзді $4 \times 16 = 64$ квартири, а в будинку – $64 \times 8 = 512$ квартир. Отже, в мікрорайоні $512 \times 20 = 10240$ квартири. Для їх обслуговування до кожного будинку підводиться десять зі 160-ти оптичних потоків рівня *STM-1*, кожен з яких зводиться до відповідного під'їзду. У під'їздах кожен потік рівня *STM-1* подається на вхід оптичного приймача для оптико-електронного перетворення. Цими приймачами в будинках закінчується оптичне мережеве обладнання. На виході кожного приймача виходить потік відеоімпульсів зі швидкістю передачі 155,52 Мбіт/с, який далі демультимплексується в 64 потоки *E1*. Ці потоки розлучаються по поверхах, а на поверхах – по квартирах абонентів.

Такий спосіб використання обладнання технології *CWDM* на ОМД є недостатньо ефективним. Найважливішою характеристикою гібридної мережі є її здатність до масштабування, тобто до нарощування пропускної здатності мережі за потреби вже в процесі її експлуатації практично без заміни та збільшення складу використовуваного обладнання. Створення гібридної мережі – це найкращий спосіб збільшення числа оптичних трактів (ОТр) між пунктами доступу (ПД), тобто збільшення пропускної здатності між цими ПД без заміни та розширення складу обладнання. Зараз, коли відбувається створення гібридних мереж, доцільно застосовувати варіант

DWDM over CWDM з використанням ВОСП *CWDM* в територіально рознесених мережах доступу.

Ідея побудови такої мережі полягає в тому [рис. 2], що по одному ОТр ВОСП *CWDM* передаються сигнали декількох ОТр, що отримані за допомогою деякої ВОСП *DWDM* з розносом між сусідніми ОТр 100 ГГц (0,8 нм). На мережах ОМД протяжністю понад 100 км можливе застосування волоконне оптичних підсилювачів (ВОП) для збільшення ділянок посилення (ПД). При цьому кожен ОТр ВОСП *CWDM* заповнюється сигналами 10 ОТр технологією ВОСП *DWDM*.

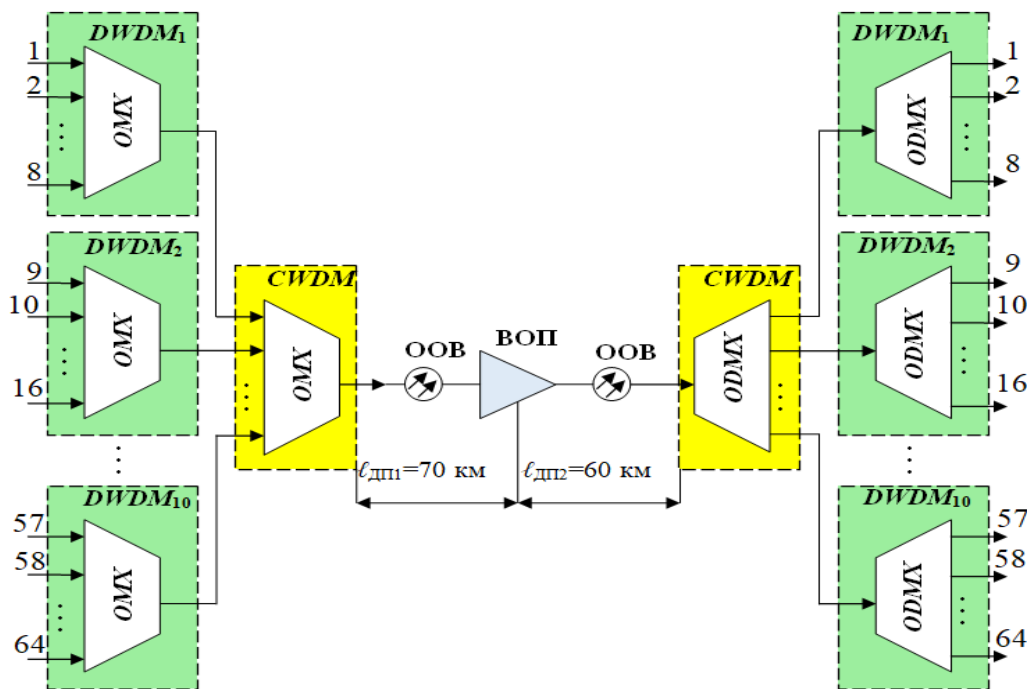


Рис. 2. Інтеграція мереж різних рівнів при використанні технології *DWDM over CWDM*.

В результаті пропускна здатність ОВ зростає в 10 разів. Наприклад, по 10 ОТр технології *CWDM* передавалися десять сигналів технології *SDH* рівня STM-64 (10 Гбіт/с), що забезпечувало пропускну здатність ОВ 100 Гбіт/с. При використанні комбінованої технології *DWDM over CWDM* утворюється всього 100 ОТр з розносом 100 ГГц (0,8 нм). Якщо по кожному з них транспортувати навантаження різних технологій (10GbE, IP, SDH) зі швидкістю передачі 10 Гбіт/с, то пропускна здатність волокна складе 1 Тбіт/с.

У ВОСП СУ кожен ОТр фактично являє собою віртуальне волокно, що утворить реальне середовище передачі оптичного сигналу на заданій довжині хвилі. У ОМД, в яких використовується технологія *DWDM over CWDM*, що утворюють ОТр на довжинах хвиль $\lambda_1, \lambda_2, \dots, \lambda_M$, практично створюються M реальних оптичних мереж.

Література

1. Хмелев К.Ф. Основы фотонного транспорта. – Киев: Техніка. 2008. – 680 с.
2. Буханець О.С., Бердников О.М. Максимальне наближення швидкостей передачі ВОСП ХМ до граничних меж. XIV Міжнародна науково-технічна конференція "Перспективи телекомунікацій" ПТ-2020: Збірник матеріалів конференції. – К.: КПІ ім. Ігоря Сікорського, 2020. – С. 62...64.

АНАЛІЗ АТАК В ПРОГРАМНО-КЕРОВАНИХ МЕРЕЖАХ

Уривський Л.О., Могилевич В.Д.

Навчально-науковий інститут телекомунікаційних систем КПІ імені Ігоря Сікорського, Україна

E-mail: vadym.vadym63@gmail.com

ANALYSIS OF ATTACKS IN SOFTWARE-DEFINED NETWORKS

The study is devoted to the analysis of typical attacks that can occur in the environment of software-controlled networks. In the context of the rapid development of SDN technologies, where network management is separated from the physical infrastructure and performed programmatically, new challenges arise in ensuring security and protecting network resources.

Постановка задачі. Програмно-керовані мережі (SDN) спрямовані на усунення проблем традиційних мереж (неефективне управління, загрози безпеці, стагнація інновацій через збільшення кількості користувачів, поява динамічних додатків та технологій гетерогенного доступу).

Основна ідея SDN [1, 2] полягає у відокремленні площин керування та передачі даних від мережевих пристроїв.

Площина управління виводиться з комутаторів і консолідується в логічно централізованому контролері. Контролер має інформацію про всю керовану мережу. Комутатори працюють як елементи переадресації і є програмованими. Вони можуть бути запрограмовані для різних цілей за допомогою мережевих додатків, що реалізовані на контролері. Комутатори, кінцеві хости та зв'язки між ними разом утворюють площину даних. Контролер з об'єднаною площиною управління - це або окремий сервер, або група логічно централізованих, але розподілених серверів. Контролер взаємодіє з комутаторами за допомогою інтерфейсів API. У випадку декількох серверів, контролери взаємодіють один з одним за допомогою східних та західних інтерфейсів. Мережеві додатки, що працюють поверх контролера, зв'язуються з ним за допомогою інтерфейсів.

Управління SDN спрямоване на вирішення різноманітних завдань, що стосуються ефективного та гнучкого керування мережевими ресурсами.

Однією з основних переваг SDN є централізоване управління мережевими ресурсами. Замість розподіленого управління на окремих мережевих пристроях, SDN дозволяє централізовано керувати всією мережею через центральний контролер.

SDN забезпечує платформу для розробки додатків безпеки та управління. Дослідники використовують цей аспект SDN для розробки різних фреймворків безпеки. Аналіз науково-технічної літератури показав,

що безпеці самої SDN не приділяється достатня увага в порівнянні з іншими дослідницькими роботами в цій області. Виклики безпеки в SDN є більш загрозливими порівняно з традиційними мережами. У традиційній мережі кілька серверів, що є частиною мережі стають об'єктами атак. На відміну від цього, якщо зловмисники компрометують площину управління SDN, під загрозою опиниться вся керована мережа [3, 4].

Отже, метою дослідження є аналіз та класифікація атак на програмно-керовану мережу.

Результати аналізу атак в мережі SDN.

Можна виділити такі загрози площини управління в SDN:

1. Несанкціонований доступ до контролера. Зловмисники можуть намагатися отримати несанкціонований доступ до контролера SDN, щоб отримати контроль над мережею і впливати на рішення, прийняті контролером.

2. Атаки на протоколи комунікації. Зловмисники можуть атакувати протоколи комунікації, використані в SDN, наприклад, OpenFlow, для впливу на трафік або виконання небажаних дій.

3. Використання вразливостей програмного забезпечення контролера. Наявність вразливостей у програмному забезпеченні контролера може використовуватися зловмисниками для виконання атак, таких як впровадження шкідливого коду або використання вразливостей для незаконного доступу.

4. Атаки на протоколи автентифікації. Зловмисники можуть намагатися атакувати протоколи автентифікації, використані в SDN, для отримання несанкціонованого доступу до системи інтелектуального управління мережею.

5. Атаки на апаратне забезпечення. Зловмисники можуть використовувати атаки на апаратне забезпечення, такі як фізичні атаки або використання вразливостей апаратного забезпечення, для отримання несанкціонованого доступу до контролера або підміни компонентів мережі.

6. Соціально-інженерні атаки. Зловмисники можуть використовувати соціально-інженерні методи, щоб отримати доступ до конфіденційної інформації або впливати на користувачів SDN, наприклад, шляхом фішингу або імітації привілейованих осіб.

Атаки на площину даних в SDN можуть включати наступні види загроз:

1. Атаки на протоколи комутації: атаки, спрямовані на протоколи комутації, такі як OpenFlow, можуть призвести до впливу на шляхи маршрутизації та пересилання даних у мережі SDN. Основне призначення OpenFlow полягає у розмежуванні логіки керування та обробки пакетів, що дозволяє розділити мережевий контроль на централізований контролер та розподілені комутатори.

Завдяки протоколу OpenFlow, контролер SDN може динамічно керувати маршрутизацією трафіку в мережі, встановлюючи правила потоків (flow rules) на комутаторах. Ці правила вказують комутаторам, які дії вони мають виконувати з пакетами даних, що надходять до них. Наприклад, контролер може встановлювати правила, які вказують комутаторам, яким шляхом маршрутизувати певний тип трафіку або як обробляти пакети в залежності від їх характеристик або вмісту.

Цей підхід дозволяє мережі бути більш гнучкою та динамічною, оскільки правила потоків можуть бути змінені або оновлені централізовано з контролера без необхідності налаштовувати кожен комутатор окремо. Крім того, використання протоколу OpenFlow дозволяє реалізувати більш складні стратегії та забезпечує більший рівень автоматизації управління мережею.

2. Атаки на вузли комутації. Ці атаки спрямовані на вузли комутації, які керують обробкою пакетів даних у мережі SDN. До таких атак можна віднести атаки на самі вузли комутації (зловмисники можуть намагатися використовувати вразливості в програмному або апаратному забезпеченні) або на їхнє фізичне середовище. До типових атак на фізичний рівень вузлів комутації SDN можна віднести:

Вплив на фізичні з'єднання та фізичне руйнування вузлів комутації: зловмисники можуть спробувати фізично пошкодити або знищити комутатори та кабелі зв'язку, що може призвести до втрати зв'язку та зниження доступності мережі.

Спроби фізичного доступу: атаки можуть включати спроби фізичного доступу до комутаторів з метою незаконного внесення змін у їхню конфігурацію, підключення шкідливих пристроїв або перехоплення мережевого трафіку.

Атаки на фізичний канал зв'язку: зловмисники можуть спробувати перехопити або модифікувати фізичний канал зв'язку між комутаторами або між комутаторами та контролером SDN, наприклад, шляхом використання атак на кабелі зв'язку.

Зловживання фізичними портами: зловмисники можуть намагатися зловживати фізичними портами комутаторів, наприклад, підключенням до них шкідливих пристроїв або спробами отримати несанкціонований доступ до мережі.

Атаки на канал зв'язку (перехоплення): зловмисник може перехопити (щоб отримати доступ до конфіденційної інформації) або модифікувати (щоб змінити маршрутизацію трафіку) трафік між контролером SDN та вузлом комутації.

Відмова в обслуговуванні (DoS): зловмисник може перевантажити вузол комутації фальшивим трафіком, щоб зробити його недоступним для законних користувачів.

Атаки на тунелювання даних: у мережах SDN можуть використовуватися тунелювання для передачі даних між вузлами. Зловмисники можуть намагатися перехоплювати або модифікувати дані, що передаються через ці тунелі, або використовувати їх для здійснення атаки на внутрішню мережу.

3. Атаки на контролер: зловмисник може намагатися атакувати контролер SDN, який керує всією мережею, шляхом використання вразливостей в програмному забезпеченні або переповнення буферів. Це може призвести до збоїв у роботі мережі та втрати контролю над мережею.

4. Атаки на мережеві пристрої: зловмисник може намагатися атакувати мережеві пристрої, такі як файрволи, перехоплювачі пакетів або мережеві монітори, щоб отримати доступ до конфіденційної інформації або вплинути на роботу мережі.

5. Атаки на шифрування даних: зловмисник може намагатися атакувати шифрування даних, що передаються через мережу SDN, для отримання несанкціонованого доступу до конфіденційної інформації або впливу на роботу мережі.

Висновки. Програмно-керовані мережі, як і будь-які інші мережеві середовища, піддаються різноманітним атакам з боку зловмисників.

Основні типи атак в програмно-керованих мережах включають атаки на контролери мережі, перехоплення пакетів, введення некоректної інформації у потокові таблиці, використання вразливостей в програмному забезпеченні та багато інших.

Важливою частиною управління програмно-керованими мережами є розуміння потенційних ризиків та вчасна реакція на атаки шляхом вдосконалення захисних механізмів та використання сучасних технологій кібербезпеки.

Ідентифікація та дослідження атак в програмно-керованих мережах є актуальним та важливим напрямком у галузі кібербезпеки і вимагає подальших досліджень для розробки нових методів захисту та забезпечення стабільності цих мереж.

Література

1. Goransson P., Black C. Software Defined Networks. A Comprehensive Approach: training manual. Publisher Morgan Kaufmann, 2014. – 352 p.
2. Software-Defined Networks. A Systems Approach: training manual / Systems Approach LLC, 2020. – 194 p.
3. Abdulsamad A.A., Salih, T.A. IoT security improvement based on SDN Controller. Eurasian Journal of Engineering and Technology, 2023. № 14. 49 – 56. URL: <https://geniusjournals.org/index.php/ejet/article/view/3199>.
4. Sheng C., Bai J. Sun Q Software-Defined Wide Area Network Architectures and Technologies: training manual. CRC Press, 2013 . – 460 p.

RELIABLE INFORMATION TRANSMISSION IN 3GPP STANDARDS FOR IOT SOLUTIONS

Tysak V., Osypchuk S.

*Educational and Scientific Institute of Telecommunication
Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: serg.osypchuk@gmail.com, valentinka.t28@gmail.com*

ДОСТОВІРНЕ ПЕРЕДАВАННЯ ІНФОРМАЦІЇ У СТАНДАРТАХ 3GPP ДЛЯ РІШЕНЬ ІОТ

У роботі розглядаються методи забезпечення надійності передачі інформації в стандартах 3GPP, а саме LTE-M та NB-IoT для рішень IoT. Запропоновано функціонал для досягнення максимальної надійності передачі інформації, відстані та швидкості передачі даних для додатків IoT.

The thesis examines techniques for ensuring information transmission reliability in 3GPP standards, namely, LTE-M and NB-IoT for IoT solutions. The functionality for achieving maximum reliability of information transmission, distance, and data transmission speed for IoT applications is proposed.

The 3rd Generation Partnership Project (**3GPP**) collaborates with telecommunications standards organisations to develop mobile communication technology specifications. Its best-known work is the development and maintenance of [1]:

- GSM and 2G and 2.5G standards, including GPRS and EDGE,
- UMTS and 3G standards, including HSPA and HSPA+,
- LTE and 4G standards, including LTE Advanced and LTE Advanced Pro,
- 5G NR and related 5G standards, including 5G-Advanced.

The next edition of the 3GPP 5G Advanced standard (Release 19) is expected to bring ambient IoT within 6G to increase connectivity from billions of devices to trillions [2]. “While 5G tracked cars, appliances and shipping containers, 6G will track everything in those cars, appliances and shipping containers,” Steve Statler, CMO of Wiliot [3].

3GPP specifications enable **interoperability** between devices and networks, allowing seamless communication and roaming across various cellular operators and geographical regions. This interoperability ensures that devices can communicate effectively regardless of the network they are connected to, facilitating global deployments and scalability.

The role of 3GPP on the Internet of Things (**IoT**) is significant. It develops standards and specifications that enable connectivity, interoperability, and scalability for IoT devices and applications. 3GPP also plays a crucial role in developing standards for cellular technologies, including **LTE-M** (LTE for Machines) and **NB-IoT** (Narrowband IoT, LPWAN), which are *optimised for IoT applications*. These standards provide a *reliable and efficient connectivity solution*

for many IoT devices, from sensors and actuators to smart meters and wearables.

LTE-M [4] (also LTE-MTC and LTE Cat M) is a Low-Power Wide-Area Network (LPWAN) technology that allows the reuse of an LTE installed base with extended coverage. LTE-M, which stands for LTE-Machine Type Communication (MTC), was also developed by 3GPP to enable devices and services specifically for IoT applications. LTE-M offers a data rate of 1Mbps for 3GPP Release 13, rising to 4Mbps for Release 14, with greater mobility and voice capability over the network.

Table 1. Techniques for achieving reliable information transmission in wireless communication systems built based on 3GPP standards for IoT systems.

Radio Channel Characteristic	Description	LTE-M	NB-IoT
Channel Coding Type, C	Error correction coding is used to improve the reliability of data transmission by taking some channel resources.	Turbo codes, LDPC (Low-Density Parity-Check)	Turbo codes, LDPC (Low-Density Parity-Check)
Multiposition Keying, M	The modulation technique is used to encode digital data into the carrier signal.	QPSK, 16/64-QAM	QPSK
Power Control Algorithms, P	Algorithms are used to adjust transmit power levels dynamically to optimise signal quality and coverage.	Power control algorithms to optimise coverage and minimise interference in varying network conditions.	Utilises power control algorithms to conserve battery power and extend device battery life in IoT deployments.
Frequency Channel Width, F	Width of the frequency channel allocated for communication.	1.4 MHz, 3 MHz, 5 MHz, 10 MHz, or 20 MHz	From 180 kHz to 3 MHz, optimised for low-power, wide-area coverage.
Frequency Band	Frequency range within the electromagnetic spectrum used for wireless communication.	700 MHz, 800 MHz, or 1.8 GHz bands	800 MHz, 900 MHz, or 1.9 GHz
Maximum Data Rate, V	Maximum achievable data transmission rate supported by the radio channel.	Up to 1 Mbps, depending on channel bandwidth and network conditions.	Up to 250 kbps, optimised for low-power, low-complexity IoT applications.
Operational Distance, L	Maximum distance over which reliable communication can be maintained.	Several kilometres, making it suitable for applications requiring wide-area connectivity.	A few kilometres, optimised for long-range communication in low-power IoT deployments.

NB-IoT [4] (Narrowband IoT) is a radio technology deployed over mobile networks which is especially suited for indoor coverage, low cost, long battery life, and many devices. NB-IoT limits bandwidth to a single narrow band of 200kHz, offering peak downlink speeds of 26kbs in Release 13 of the 3GPP standard. Release 14 will see this increase to 127kbps.

Table 1 outlines the wireless radio channel characteristics and techniques for LTE-M and NB-IoT radio channel specifications for achieving low BER and high information transmission reliability.

Reliable information transmission refers to the ability of a communication system to deliver data accurately and consistently from a sender to a receiver, even in the presence of various impairments and challenges that can degrade the quality of the transmission. It has such characteristics as *accuracy, consistency, robustness, and timeliness*. In a reliable transmission, the information arrives at the receiver with *minimal errors* (low bit error rate, BER) or distortions, ensuring the intended message is *accurately conveyed and interpreted* on the recipient side. Reliable information transmission is usually a *pain point of wireless communication channels* rather than wired ones.

Mathematical functional for minimising BER and maximising distance L and data rate V depend on and proportional to parameters combination set such as coding type C and its rate, multiposition keying M, frequency band F, and transmitter power P:

$$\left\{ \begin{array}{l} \min BER \\ \max L \\ \max V \end{array} \right\} \propto \{C, M, F, P\}$$

Calculation of the NB-IoT and LTE-M link budget is defined in the Study on the channel model for frequencies from 0.5 to 100 GHz (3GPP TR 38.901 version 17.1.0 Release 17), ETSI TR 138 901 V17.1.0 [5].

Thus, this work shows that modern 3GPP communication standards and technologies such as LTE-M and NB-IoT have sufficient technical capabilities for building reliable networks to serve IoT traffic and applications. Further research in the scope of this work is supposed to calculate the coverage zones for both technologies based on the link budget and variety of channel parameters following the proposed mathematical functional, as well as other link budget parameters.

References

1. Third Generation Partnership Project Agreement, <http://www.3gpp.org>
2. Predictions for 2024 – 3GPP and Ambient IoT <https://www.electronicweekly.com>
3. Wiliot Cloud and IoT, <https://www.wiliot.com>.
4. LTE-M vs NB-IoT – A Guide Exploring the Differences between LTE-M and NB-IoT, <https://iot.telenor.com/iot-insights/lte-m-vs-nb-iot-guide-differences>
5. Study on channel model for frequencies from 0.5 to 100 GHz (3GPP TR 38.901 version 17.1.0 Release 17), ETSI TR 138 901 V17.1.0 (2024-01), <https://www.etsi.org>

INFORMATION TRANSMISSION PROBLEMS IN DUAL-PURPOSE IOT SOLUTIONS

Klishchuk V., Osypchuk S.

National Technical University of Ukraine

“Igor Sikorsky Kyiv Polytechnic Institute”

E-mail: serg.osypchuk@gmail.com, vkishchuk@gmail.com

ПРОБЛЕМИ ПЕРЕДАВАННЯ ІНФОРМАЦІЇ В РІШЕННЯХ ІОТ ПОДВІЙНОГО ПРИЗНАЧЕННЯ

Our research delves into the crucial realm of IoT dual-purpose systems (DPS). We meticulously analyse the information transmission problems (ITP) in IoT DPS and provide a comprehensive list of techniques to mitigate them. We also present a high-level design of wearable health monitoring devices and a network diagram, showcasing one of the many applications of IoT DPS.

Internet of Things (IoT) refers to the network of physical objects or "things" embedded with sensors, software, and other technologies that enable them to connect and exchange data with other devices and systems over the Internet without human intervention.

The dual-purpose system (DPS) is designed to serve two distinct functions or purposes simultaneously.

IoT DPS, which can serve personal, industrial, or enterprise applications, is crucial in various fields, including engineering, healthcare, or military applications. By combining multiple capabilities of IoT applications into a single solution, IoT DPSs enhance efficiency and flexibility, thereby optimising resources and functionality. This is particularly significant in the face of increasing risks of conflicts and threats, underscoring the importance of IoT DPS research and development. *Table 1* showcases examples of IoT DPS designed explicitly for civil and military applications, emphasising their relevance.

Information transmission problem (ITP) refers to any issue or challenge that hinders the effective and reliable transfer of information from one point to another within a system or network. ITP can arise due to various factors, such as *technical limitations, environmental conditions, security concerns, or protocol inefficiencies*.

The *relevance of IoT DPS research and development* is the increased risks of conflicts and threats nowadays. Thus, proper attention must be paid to addressing the ITPs in IoT DPSs. *Table 2* shows critical ITPs in IoT DPSs.

Addressing ITP often requires developing and implementing appropriate technologies, protocols, and strategies tailored to the specific requirements and constraints of the communication system or network.

Task statement. The objective is to address the urgent need to reduce risks in military and civilian cases that could lead to lethal results: review the *wearable health monitoring devices (WHMD)* scenario [1-3]. This will be achieved by applying techniques for addressing ITPs in the IoT DPS listed in *Table 2*.

Table 1. Examples of the IoT DPS.

№	Dual-purpose system (DPS)	Civil Application	Military Application
1	Wearable health monitoring devices	Monitoring of vital signs, activity levels, sleep, patterns for patients with chronic conditions, fitness, tracking for wellness purposes	Remote health monitoring of soldiers in the field, tracking physiological indicators during missions, assessing fatigue and stress levels
2	Unmanned aerial vehicles (UAVs) or Drones	Aerial photography, mapping, surveillance, monitoring of infrastructure, agriculture, environmental conditions	Intelligence, surveillance, reconnaissance, target acquisition, battlefield situational awareness
3	Smart city infrastructure	Urban management, traffic control, public safety, environmental monitoring, energy efficiency	Critical infrastructure protection, emergency response coordination, support for military installations
4	Border surveillance systems	Border security, customs enforcement, monitoring of immigration, cross-border movements	Border control, intelligence gathering, detection of illicit activities, prevention of unauthorised incursions
5	Emergency response and disaster management	Early warning systems, disaster preparedness, search and rescue operations, humanitarian assistance	Rapid deployment of forces for disaster relief, coordination of emergency response efforts

Table 2. Information transmission problems (ITP) in the IoT DPS.

№	ITP	Challenges	Techniques for addressing ITP
1	Communication channel noise and signal interference, reliability, and error correction	External factors that distort or corrupt the transmitted signals, leading to errors in data reception, reliable data transmission	Channel coding, error detection and correction, modulation techniques and multiposition keying (MPK), antenna diversity, frequency hopping spread spectrum (FHSS), adaptive filtering, cyclic redundancy check (CRC), OFDM, dynamic spectrum access, automatic/selective/hybrid repeat request (ARQ), LDPC codes, interleaving, concatenated coding, soft decision decoding, iterative decoding, and combinations of these techniques
2	Security threats	Unauthorised access to the data, confidentiality breach of the transmitted data, data integrity or availability	Data encryption (AES, RSA, ECC), authentication and authorisation, keys management, secure protocols (TLS, IPSec, SSH, HTTPS), firewalls, intrusion detection systems (IDS), packet filtering, traffic analysis, virtual private networks (VPN), secure network design (segmentation, least privilege access)
3	Reliable design	Lack of shockproof, waterproof, autonomous power for long-lasting work	Shock-absorbing materials, vibration-dampening mounts, solder joints and connectors, sealed enclosures, energy harvesting, energy-efficient components, economic power-management system, battery backup to allow communication to continue

The WHMD solution involves attaching IoT sensors to human individuals to collect telemetry data, encrypting and transmitting that information to storage facilities and to authorised personnel. Advances in Microelectromechanical Systems (*MEMS*) technology have resulted in the development of small and robust sensors that can monitor various parameters such as human movement, temperature, and others. The modern concept of Wireless Body Area Sensor Networks (*WBASN*) allows the integration of different networks and devices for remote monitoring. The WBASN structure consists of three *key stages* (Figure 1):

1. Data gathering about and around the human body.
2. Communication between humans and the command centre via ZigBee, Bluetooth, UWB, IEEE 802.11 a/b/g/n/ah WLAN, and 3G/4G cellular technologies at different steps of network design.
3. The overall WHMD communication scenario is managed by appropriately reacting to the gathered data.

All the ITP problems in Table 2 are applicable to this IoT DPS WHMD use case, and proper techniques for addressing ITP can be used.

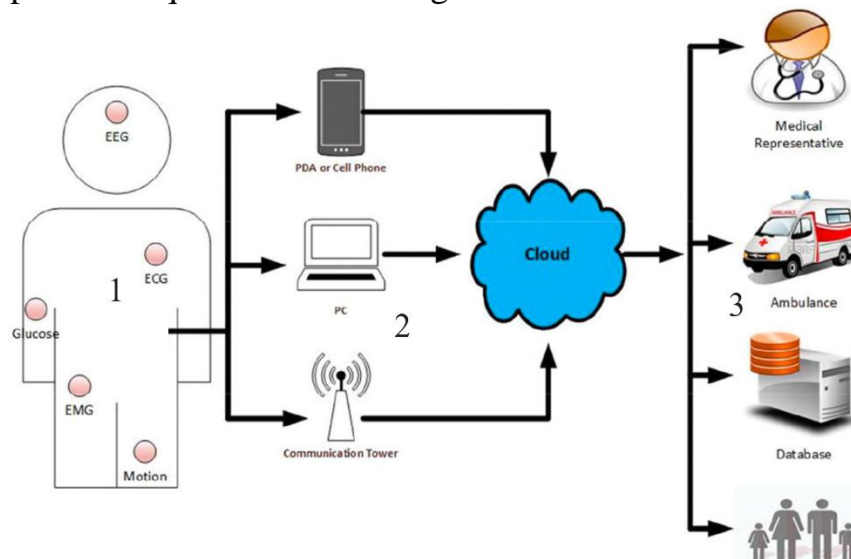


Figure 1. WBASN communication scheme.

In conclusion, our research has shown that IoT dual-purpose systems must be appropriately designed considering existing threats worldwide. By doing so, we can create reliable solutions with cost savings, eliminating the need to develop different systems. Our research provides techniques for addressing common information transmission problems.

References

1. Al Ameen, M., Liu, J. & Kwak, K. Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications. *J Med Syst* 36, 93–101 (2012). <https://doi.org/10.1007/s10916-010-9449-4>.
2. Khan RA, Pathan A-SK. The state-of-the-art wireless body area sensor networks: A survey. *International Journal of Distributed Sensor Networks*. 2018; 14(4). <https://journals.sagepub.com/doi/10.1177/1550147718768994>.
3. Bin Ahmad, M., Asif, M., Masood, K., Al Ghamdi, M. A., Almotiri, S. H., & Nagra, A. A. (2022). A Reliable Framework for Secure Communication and Health Assessment of Soldiers in the Battlefield. *Sage Open*, 12 (4). <https://doi.org/10.1177/21582440221130300>.

ПРОТОКОЛИ РІВНЯ ЗАСТОСУНКІВ В МЕРЕЖАХ ІоТ

Григоренко О.Г., Дідковська Н.А.

Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: olenagri@ukr.net, didkovska.natalia@ill.kpi.ua

APPLICATION LAYER PROTOCOLS IN ІоТ NETWORKS

The main application protocols in the Internet of Things networks are analyzed and their features are defined, which should meet the functional requirements and basic characteristics of IoT devices that exchange information.

Проаналізовані основні протоколи рівня застосунків в мережах Інтернету речей та зазначені їх особливості, що повинні відповідати вимогам функціонування і основним характеристикам пристроїв ІоТ, які обмінюються інформацією.

Останнім часом кількість пристроїв Інтернету Речей (ІоТ) збільшується з вражаючою швидкістю, що відкриває безліч перспектив для подальшого розвитку людства. Це потребує ефективних протоколів на рівні застосунків, сервісів, інфраструктури, що відповідають потребам пристроїв ІоТ, які характеризуються обмеженими ресурсами: мале споживання енергії, малий обсяг пам'яті та трафіку, що генерується, простота та інші. Дану мережу можна порівняти з лабіринтом, адже Інтернет речей – це велика кількість протоколів, які визначають, як пристрої спілкуються, обмінюються даними і взаємодіють у мережі. Протоколи рівня застосунків в мережах ІоТ визначають способи, за якими пристрої збирають, обробляють та передають дані, відкриваючи безмежні можливості для покращення нашого повсякденного життя та розвитку промисловості. Нижче проаналізовані особливості та характеристики протоколів рівня застосунків, що найчастіше використовуються у Інтернеті речей, зазначені їх переваги та недоліки, проведено порівняння.

MQTT (Message Queuing Telemetry Transport) — це відкритий стандартний протокол обміну повідомленнями, реалізований OASIS і рекомендований Міжнародною організацією зі стандартизації (ISO/IEC 20922). Він розроблений як надзвичайно легкий засіб для обміну повідомленнями за допомогою публікації/підписки на сервері-брокері в мережах M2M (machine-to-machine), ідеально підходить для підключення віддалених пристроїв з невеликим кодовим простором і мінімальною пропускнуою здатністю мережі, що відповідає характеристикам пристроїв ІоТ. Сьогодні MQTT використовується в найрізноманітніших галузях, таких як автомобілебудування, виробництво, телекомунікації, нафтогазова промисловість тощо. Переваги даного протоколу включають в себе [1]:

1. MQTT дозволяє обмінюватися повідомленнями між пристроєм у хмару та з хмари на пристрій. Це спрощує трансляцію повідомлень групам речей.

2. Масштабування MQTT для підключення до мільйонів пристроїв IoT.

3. Надійна доставка повідомлень.

4. Підтримка трьох класів якості обслуговування QoS.

5. Підтримка ненадійних мереж: Багато пристроїв IoT підключаються через ненадійні стільникові мережі. Підтримка MQTT для постійних сесій скорочує час на повторне з'єднання клієнта з брокером.

6. Безпека протоколу: MQTT дозволяє легко шифрувати повідомлення за допомогою TLS і автентифікувати клієнтів за допомогою сучасних протоколів автентифікації, таких як OAuth. Є можливість налаштування процесу відстеження всіх станів підключення клієнта, включаючи облікові дані безпеки та сертифікати.

В якості недоліків можна відмітити, що безпека протоколу була скомпроментована у 2020 р. [6] (CVE-2020-13849). Також наявність брокера, через який відбувається обмін повідомленнями, є “слабким” місцем мережі при перериванні обслуговування. Проте вбудована черга брокерів MQTT може в такій ситуації забезпечити буферизацію для обмежених пристроїв IoT, які не мають можливості зробити це самостійно.

HTTP (Hypertext Transfer Protocol) - протокол передачі гіпертексту є основою Інтернету і використовується для завантаження веб-сторінок за допомогою гіпертекстових посилань [2]. Призначений для передачі інформації між мережевими пристроями на прикладному рівні моделі OSI та працює поверх інших рівнів стека TCP/IP. Типовий потік через HTTP передбачає, що клієнтська машина робить запит до сервера, який потім надсилає повідомлення у відповідь. HTTP, як правило, розроблений таким чином, щоб бути простим і зручним для читання людиною, навіть з урахуванням додаткової складності, яка притаманна HTTP/2, шляхом інкапсуляції повідомлень у фрейми. Зрозумілість HTTP-повідомлень полегшує тестування для розробників і знижує складність для новачків. З'єднання контролюється на транспортному рівні, і тому принципово виходить за рамки HTTP. Він не вимагає, щоб базовий транспортний протокол був заснований на з'єднанні, лише щоб був надійним, або не втрачав повідомлення (як мінімум, представляючи помилку в таких випадках). Тому HTTP працює поверх TCP. [3]

CoAP (The Constrained Application Protocol) — це легкий протокол, призначений для використання з пристроями з низьким енергоспоживанням, обчислювальною потужністю, пам'яттю та часом автономної роботи, такими як пристрої IoT, і обмеженими пропускнуою здатністю мережами. Визначає протокол веб-передачі на основі репрезентативного стану (REST) на додаток до функцій HTTP, це надає простіший спосіб обміну даними між клієнтами та серверами через HTTP. CoAP спирається на архітектуру клієнт-сервер без збереження стану. Він використовується в мобільних додатках і програмах соціальних мереж і усуває неоднозначність за допомогою методів HTTP get, post, put і delete. CoAP надає набір методів для виявлення, маніпулювання та моніторингу ресурсів, а також підтримку асинхронного зв'язку та кешування.

CoAP працює поверх протоколу UDP і зазвичай використовує порт 5683 для незахищеного зв'язку та порт 5684 для безпечного зв'язку за допомогою DTLS (Datagram Transport Layer Security). [4]

Основними перевагами протоколу є:

- зменшення накладних витрат на зв'язок за рахунок поблочного транспортування ресурсів, коли при обміні даними між клієнтом і сервером непотрібно оновлення всіх даних,
- гнучкість взаємодії з HTTP через проксі,
- безпека на основі DTLS.

Служба розподілу даних (DDS-Data Distribution Service) - це протокол проміжного програмного забезпечення (middleware) та стандарт API для зв'язку. Використовує механізм публікації/підписки для комунікацій M2M у реальному часі. Він об'єднує компоненти системи разом, забезпечуючи низьку затримку передачі даних, надзвичайну надійність, розширену безпеку та масштабовану архітектуру, необхідну для бізнес-додатків та критично важливих додатків Інтернету речей [5]. На відміну від інших протоколів публікації/підписки, таких як MQTT, DDS покладається на архітектуру без посередників і використовує багатоадресну розсилку, щоб забезпечити відмінну якість обслуговування (QoS) і високу надійність своїх програм. Його архітектура публікації/підписки без брокерів добре відповідає обмеженням реального часу для комунікацій IoT та M2M. DDS підтримує 23 політики QoS, за допомогою яких розробник може врахувати різноманітні критерії зв'язку, такі як безпека, терміновість, пріоритет, довговічність, надійність тощо [7].

Таблиця 1. Порівняння протоколів.

	MQTT	CoAP	DDS	HTTP
Клієнт-серверна архітектура	так	так	так	так
Механізм публікації/підписки	так	так	так	ні
Запит/відповідь	ні	так	ні	так
Транспортний протокол	TCP	UDP	TCP/UDP	TCP
Безпека	SSL	DTLS	SSL/DTLS	SSL
QoS	так	так	так	ні
Розмір заголовку (байт)	2	4	-	-

Підсумовуючи можна сказати, що проаналізовані протоколи відповідають вимогам обмеження ресурсів в пристроях і мережах IoT і знаходять застосування в різноманітних сценаріях і середовищах.

Література

1. Головний сайт MQTT <https://mqtt.org/>
2. <https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/>
3. <https://developer.mozilla.org/en-US/docs/Web/HTTP/Overview>
4. <https://cqr.company/ru/wiki/protocols/constrained-application-protocol-coap/>
5. <https://www.twinoakscomputing.com/datasheets/DDS-Brochure.pdf>
6. Vaccari, I., Aiello, M., & Cambiaso, E. (2020). SlowITe, a novel denial of service attack affecting MQTT. *Sensors*, 20(10), 2932.
7. <http://www.omg.org/>

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ ІоТ В ПРОМИСЛОВОСТІ

Григоренко О.Г., Петренко В.О.

*Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: olenagri@ukr.net, petrenko.vladislava@ill.kpi.ua*

USE OF IoT TECHNOLOGY IN INDUSTRY

The indicated use areas of the Internet of Things and the analyzed features of the industrial Internet of Things on the example of Smart grid and the advantages of using.

Зазначені галузі використання Інтернету речей та проаналізовані особливості промислового Інтернету речей на прикладі “розумних” енергомереж (Smart grid) та переваги використання.

Використання технології Інтернету речей стало повсякденним атрибутом нашого життя. “Розумні” речі використовуються в багатьох галузях промисловості, в медицині, сільському господарстві, енергетиці, транспорті, торгівлі, телекомунікаціях і ІТ-секторі, уряді, у сфері банківської справи, фінансових послуг та страхування (BFSI), освіти тощо. За оцінками експертів ринок Інтернету Речей (IoT) і надалі буде невпинно зростати. За прогнозами [1] очікується, що кількість встановлених підключень IoT швидко зростатиме протягом десятиліття і у 2033 році складе 39,5 білліон пристроїв. Ця кількість, крім сенсорів і пристроїв IoT, включає також пов’язані пристрої агрегації (рис.1).

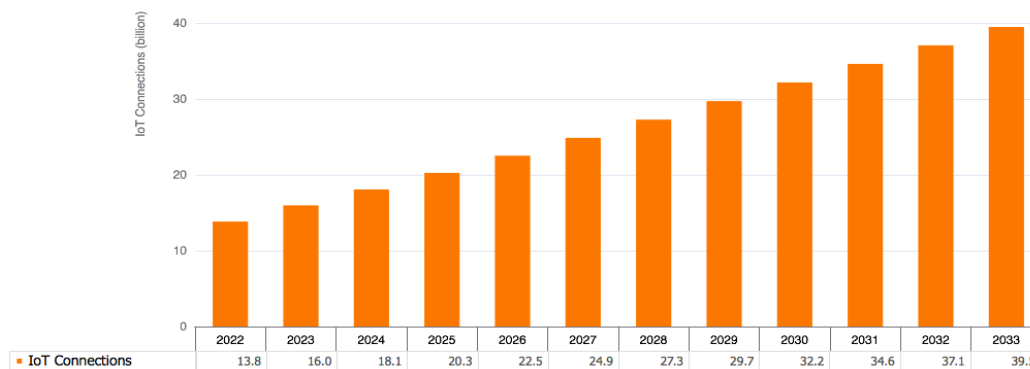


Рис.1. Кількість підключень сенсорів і пристроїв IoT, враховуючи пристрої агрегації, за роками [1].

Також можна зазначити, що за даними аналізу світового ринку використання IoT [2], найбільша частка пристроїв IoT припала на галузь охорони здоров'я (19,7%), транспорт, сектор ІТ та телекомунікацій і т.д. (рис.2).

Однією із складових Інтернету речей є промисловий, або індустріальний, Інтернет речей, який представляє собою систему об'єднаних комп'ютерних мереж і підключених до них промислових (виробничих) об'єктів з вбудованими датчиками і програмним забезпеченням для збору та

обміну даними, з можливістю віддаленого контролю і управління в автоматизованому режимі, без участі людини [3]. Нижче проаналізовані особливості промислового Інтернету речей на прикладі “розумних” електромереж (Smart grid) та переваги використання.

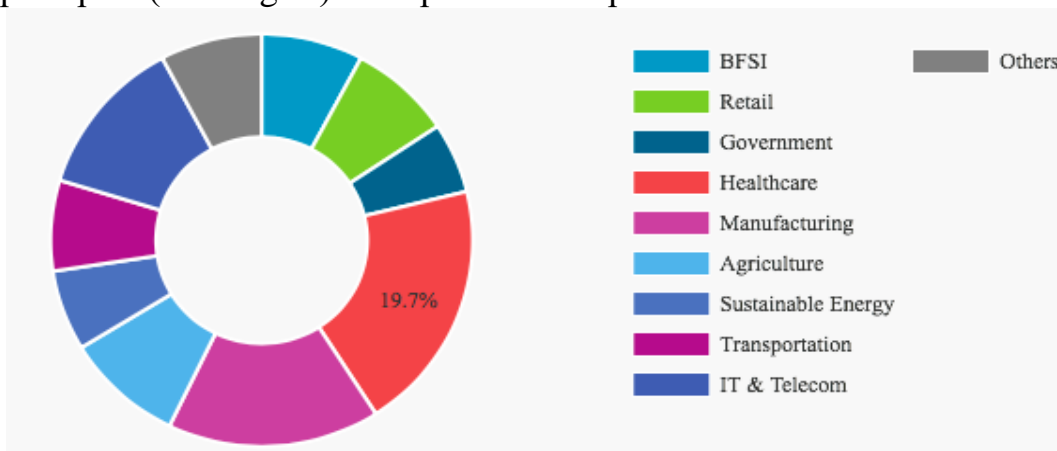


Рис. 2. Частка світового ринку за галузями кінцевого використання, 2023 [2].

При впровадженні промислового IoT устаткування обладнується датчиками, виконавчими механізмами, контролерами та відповідними інтерфейсами, через які збирається інформація. Отримані результати обробляються і приймаються обґрунтовані виробничі рішення, що допомагають уникнути позапланових простоїв, несправностей обладнання, збоїв в управлінні ланцюжками постачання, тобто підприємство працює більш ефективно.

При обробці величезного масиву неструктурованих даних, що надходять з датчиків, їх фільтрація і адекватна інтерпретація стає пріоритетним завданням. Аналітичні платформи, що використовуються для збору, зберігання і аналізу даних повинні працювати в режимі реального часу. Використання IoT робить підприємства більш ощадливими, гнучкими і ефективними. В міру становлення цифрових екосистем виробничі підприємства з ізольованих систем, які самостійно виконують всі необхідні для виробництва продукції виробничі та бізнес-процеси, перетворюються у відкриті системи, що поєднують різних учасників ринку; а засобами виробництва в цих системах управляють хмарні сервіси, і кінцевою метою всіх цих трансформацій є надання послуг споживачеві.[3]

“Розумна” електромережа (Smart grid) — це нова сучасна електромережа, яка добре інтегрована з передовою технологією вимірювання датчиків, інформаційно-комунікаційними технологіями, технологією аналізу прийняття рішень, технологією автоматичного керування, технологією енергетики та мережевою інфраструктурою. Порівняно з традиційною електромережею, інтелектуальна мережа значно вдосконалена в оптимізації контролю потужності, гнучкості структури мережі, оптимізації розподілу ресурсів і покращенні якості послуг електроенергії. Таким чином, розумна мережа має багато характеристик, включаючи міцність, самовідновлення, сумісність, економічність, інтеграцію та оптимізацію тощо [3,4].

В Інтернеті речей, де речі комунікують один з одним, за допомогою

певних протоколів і таких технологій IoT, як технології радіочастотної ідентифікації, сенсорні технології, інтелектуальні технології, нанотехнології, можна обмінюватися інформацією про взаємозв'язок, а також можна досягти інтелектуального розпізнавання, позиціонування, відстеження, моніторингу та управління.

IoT ефективно інтегрує ресурси інфраструктури в систему зв'язку та електроенергетики, забезпечує функціонування інформаційно-комунікаційних послуг для електроенергетичної системи, підвищує рівень інформованості енергосистеми та ефективність використання інфраструктури в існуючій енергосистемі. Оскільки технологія IoT використовується в розумних мережах, важлива технічна підтримка для генерації, передачі, функціонування підстанцій, розподілу, послуг електроенергії та інших аспектів [5].

Як приклад IoT в Smart grid на рисунку 3 показаний сценарій використання технології Інтернету речей для прогнозування енергії вітру. Це виконується головним чином через мережу бездротових датчиків (WSN), дані про вітер збираються в режимі реального часу, а зміну потужності можна передбачити.

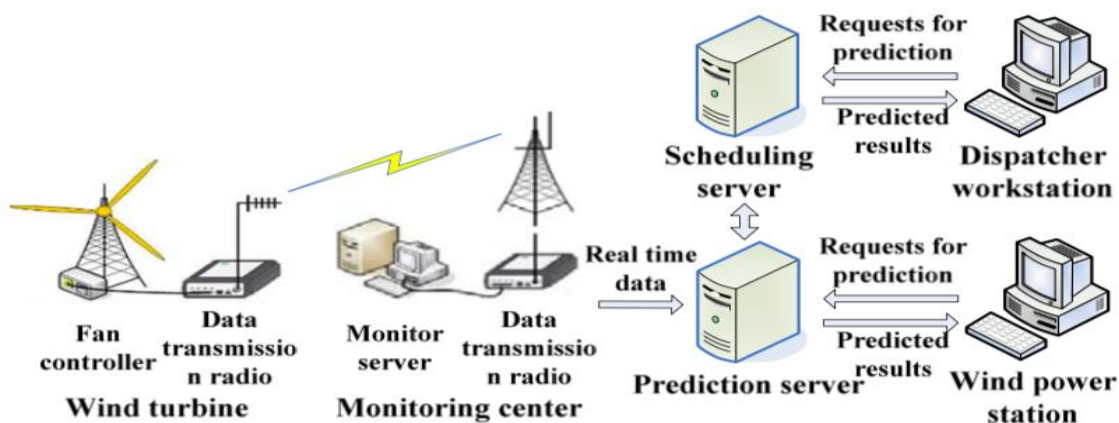


Рис.3 Прогноз енергії вітру на основі IoT [5].

Підсумовуючи можна сказати, що застосування IoT в різноманітних сценаріях і середовищах надає такі характеристики як ефективність, міцність, самовідновлення, сумісність, економічність, інтеграцію та оптимізацію тощо.

Література

1. <https://transformainsights.com/research/forecast/highlights>.
2. <https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307>.
3. <https://www.it.ua/knowledge-base/technology-innovation/promyshlennyj-internet-veschej>.
4. Chen, Z.; Amani, A.M.; Yu, X.; Jalili, M. Control and Optimisation of Power Grids Using Smart Meter Data: A Review. *Sensors* 2023,23,2118. - електронний ресурс: <https://www.mdpi.com/1424-8220/23/4/2118>.
5. Liu Hua, Zhang Junguo, Lin Fantao. Internet of Things Technology and its Applications in Smart Grid. *TELKOMNIKA Indonesian Journal of Electrical Engineering* .-Vol.12, No.2, February 2014, pp. 940 – 946.

РОЗРОБКА СИСТЕМИ ВІДДАЛЕНОЇ ДІАГНОСТИКИ АВТОМОБІЛІВ НА ОСНОВІ ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ

Хрокало О. Г., Мошинська А. В.

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна
E-mail: xrokaloc@gmail.com*

DEVELOPMENT OF A REMOTE VEHICLE DIAGNOSTICS SYSTEM BASED ON IOT TECHNOLOGIES

The variants of car diagnostics solutions are considered, the variant of remote diagnostics is proposed and its method of application is given. All modules used in the system are considered and the scheme is demonstrated. An example of why this development is needed is given.

Пристрої діагностики автомобіля набувають все більшої популярності та активного застосування в сфері ремонту та обслуговування автомобілів. Щодня технології побудови автомобілів покращуються та ускладнюються. Але більшість з них або стаціонарні і потребують перебування майстра в автомобілі або працюють на відстані не більш 10 метрів від транспортного засобу.

Частіше за все при техогляді або ремонті автомобіля використовується роз'єм OBD II. Саме завдяки тому, що у всіх автомобілях використовується ця технологія для поєднання датчиків розміщених по усьому транспортному засобу, проводиться загальний та швидкий огляд автомобіля.

На даний момент загальна спеціальність автомайстрів поділяється на напрямки в залежності від типу робіт. В залежності від розмірів та напрямків роботи автомайстри можуть займатись: електронікою, ремонтом коробок передач, обслуговуванням та ремонтом двигунів та ін. Але все починається з технічного огляду (ТО), під час якого обов'язково буде використовуватись сканування усіх частин автомобіля [1].

Для спрощення роботи майстрів та покращення умов для автомобілістів створюється прототип, який допоможе проводити діагностику роботи в реальному часі, коли автомобіль буде перебувати в дорозі, за допомогою модуля під'єднання до датчиків, мікрокомп'ютера та модуля

(GSM|GPS). Конструкція має малогабаритні розміри, легке встановлення, потребує тільки початкового налаштування та має широкий спектр вдосконалення.

Більшість автомобілів бюджетного сегменту не мають бортового комп'ютера, за допомогою якого можна було б дізнатись більше інформації для швидшого реагування та вирішення проблеми завчасно не доводячи машину до критичного стану. Дана технологія може зменшити витрати коштів та часу водіїв. Використовуючи модуль OBDII, який використовує дані в форматі числового коду та надсилає їх до мікрокомп'ютера Raspberry Pi, який переформовує цю інформацію в доступний матеріал та відтворює за допомогою застосунку. Таким чином можна в короткий термін визначити проблему, не затрачаючи великих зусиль.

Для даного прототипу можуть використовуватись стандартні протоколи GSM та Wi-Fi. Дані технології використовуються повсякденно кожним з нас, а для застосування потрібно просте підключення оператора або точки доступу, яка має доступ до мережі Інтернет.

Кожен з модулів і елементів є в доступності будь для кого, і за невеликою ціною. Їх можна придбати або замінити іншими доступними або більш новими елементами, які можуть бути оригінальними [3] або їх дешевими варіантами [2]. Підбір кожного з модулів проходить за певними критеріями які нам потрібні для роботи. Модуль OBD II має два варіанти: проводований або безпроводований (Bluetooth/Wi-Fi). За допомогою одного з варіантів буде проходити підключення до мікрокомп'ютера. Вибір модуля керування відштовхувався від можливостей цього модуля. Raspberry PI має варіанти з різними мікроконтролерами, кількістю портів, об'єм пам'яті, кількістю RAM пам'яттю, можливостями та габаритами модуля GSM.

Даний прототип використовує діагностичний OBD-II автосканер ELM327 з підтримкою з'єднання по Bluetooth [4], мікрокомп'ютер використовується Raspberry PI 4 model B на 8 Гб оперативної пам'яті, 4 роз'єми USB (2 порти type USB3 та 2 порти type USB2), порт Gigabit Ethernet, порт живлення USB-C power supply, та два роз'єми для виводу зображення micro HDMI 4K displays [5]. Також він має функціонал типу Bluetooth, Wi-Fi та інші дрібні можливості. Зверху модуля є 48 пінів (контакти) за допомогою яких можна під'єднати модулі різного типу та спрямування. До цих пінів підключається модуль зв'язку SIM7600G-H [6]. Останнє, що потрібно – це

SIM-карта одного з провайдерів телефонного зв'язку та microSD-карта яка буде накопичувачем для мікрокомп'ютера

При загальному зборі даної моделі вона матиме компактний розмір та просту схему Рис. 1.



Рис. 1. Схема роботи пристрою віддаленої діагностики автомобіля.

Для роботи пристрою встановлюється операційна система, налаштовується взаємодія модулів та використовується написаний код для зчитування інформації та передавання на кінцевий пристрій.

Даний прототип моделі віддаленої діагностики автомобіля використовує технології IoT для збору, обробки та передавання інформації на великих відстанях, що допоможе автовласникам своєчасно реагувати на проблеми автомобіля та вирішувати їх. Додатково дану технологію можна вдосконалити в залежності від потреб.

Література

1. Типи підприємств автосервісу URL: <https://studfile.net/preview/7242470/page:6/>
2. Мікрокомп'ютер Raspberry Pi URL: <https://www.raspberrypi.com/products/raspberrypi-4-model-b/>
3. Приклад модуля OBD II URL: <https://rozetka.com.ua/ua/elm-avs000001/p389331663/characteristics/>
4. DATASHEET Raspberry Pi 4 Model B Copyright Raspberry Pi (Trading) Ltd. 2024 URL: <https://datasheets.raspberrypi.com/rpi4/raspberrypi-4-datasheet.pdf>.
5. SIM7600G-H User manual URL: <https://fcc.report/FCC-ID/2AJYU-8PYA007/4857209.pdf>.

РОЗРОБКА СИСТЕМИ ДИСТАНЦІЙНОГО КЕРУВАННЯ ЕЛЕКТРОМЕРЕЖЕЮ ЖИТЛОВОГО ПРИМІЩЕННЯ НА ОСНОВІ ТЕХНОЛОГІЙ ІоТ

Голубєва М. А. Мошинська А. В.

Навчально-науковий інститут телекомунікаційних

систем КПІ ім. Ігоря Сікорського, Україна

E-mail: holubchuk292929@gmail.com

DEVELOPMENT OF A SYSTEM FOR REMOTE CONTROL OF THE RESIDENTIAL POWER GRID BASED ON IOT TECHNOLOGIES

The development of a remote control system for a building's power grid based on DTMF signals via a GSM module includes wireless network analysis, software and hardware design, economic analysis and modernization prospects, a detailed review of market analogues, a comprehensive model development and testing process, including pulse and tone dialing, with further conclusions on the efficiency, reliability and prospects for system development.

Розробка моделі системи віддаленого керування зосереджує свої зусилля на створенні системи, яка дозволить власникам житлового приміщення керувати електромережею на відстані. Основою для цього служить використання DTMF сигналів, які передаються через GSM модуль. Система має на меті забезпечити зручне та ефективне управління електроприладами, такими як освітлення, опалення та інші електричні системи в домогосподарстві, з будь-якої точки світу, де є доступ до мобільного зв'язку. Важливою частиною проекту є вибір GSM як основної технології зв'язку через її широке покриття та високу надійність, що забезпечує стабільне управління системою незалежно від місцеположення користувача.

Головною метою роботи є розробка моделі системи віддаленого керування, яка використовуватиме DTMF сигнали для управління електромережею через мобільний зв'язок. Для реалізації цієї системи обрано платформу Arduino Nano [1] та GSM модуль SIM800L[2]. Важливість цього проекту полягає у створенні доступного, надійного та легкого в управлінні рішення для автоматизації домашньої інфраструктури, що дозволить користувачам ефективно керувати енергоспоживанням, підвищити комфорт та безпеку проживання, використовуючи лише свій мобільний телефон для віддаленого доступу та керування.

У роботі проводиться детальний аналіз можливостей різних бездротових мереж, включаючи Wi-Fi, Bluetooth, NFC, ZigBee та інші, для визначення найбільш підходящої технології для віддаленого керування електромережею. Вибір падає на GSM через його універсальність, широке географічне покриття та високий рівень надійності[3]. Таке рішення забезпечує

стабільний зв'язок між системою управління та кінцевим користувачем, дозволяючи відправляти команди керування з будь-якої точки світу. Аналіз показує, що використання

стільникового зв'язку дозволяє ігнорувати потенційні обмеження, пов'язані з діапазоном дії або перешкодами для сигналу, характерними для інших бездротових технологій.

Важливою частиною проекту є розробка програмної та апаратної складових системи віддаленого керування. Основою апаратної частини виступає платформа Arduino Nano, обрана за її компактність, доступність та гнучкість у програмуванні, що дозволяє легко інтегрувати різні модулі та сенсори. GSM модуль SIM800L використовується для забезпечення мобільного зв'язку між системою та користувачем, дозволяючи відправляти DTMF команди через мережу. Програмна частина включає розробку відповідного програмного забезпечення [4] (скетчів для Arduino IDE), що дозволяє обробляти сигнали управління та виконувати задані дії, такі як вмикання або вимикання приладів. Це забезпечує гнучкість управління системою та її адаптацію під конкретні потреби користувача.

Проект також охоплює аналіз економічних аспектів розробки та впровадження системи віддаленого керування. Важливою складовою є оцінка вартості компонентів, потенційна вартість виробництва на масштабах промислового випуску та можливі економічні вигоди для кінцевих користувачів, зокрема, зниження витрат на електроенергію та підвищення комфорту використання. Окремо розглядаються перспективи подальшої модернізації системи, включаючи інтеграцію з іншими розумними домашніми системами та можливість використання новітніх технологій для розширення функціоналу.

Проведено детальний аналіз ринку існуючих рішень у сфері віддаленого керування електромережами та домашніми системами. Цей аналіз включає огляд доступних на ринку пристроїв та систем, їх функціональних можливостей, переваг та обмежень. На основі порівняльного аналізу визначено ключові відмінності розроблюваної системи від конкурентів, зокрема, в плані вартості, гнучкості та ефективності управління. Це дозволяє визначити потенційні переваги та ніші на ринку, де нова система може знайти своє застосування та користувачів.

Проектування моделі системи віддаленого керування електромережею охоплює кілька критичних етапів, починаючи з вибору елементної бази та закінчуючи розробкою детальної схеми (Рис. 1) з'єднань та програмного коду. Першочергово, враховуються потреби користувачів та специфіка використання системи, що визначає вибір апаратних компонентів, зокрема мікроконтролера Arduino Nano для керування логікою системи та GSM модуля для забезпечення зв'язку з користувачем через мобільну мережу. Розробка програмної складової включає створення скетчів для Arduino, які виконують обробку вхідних команд та управління підключеними до системи електричними пристроями

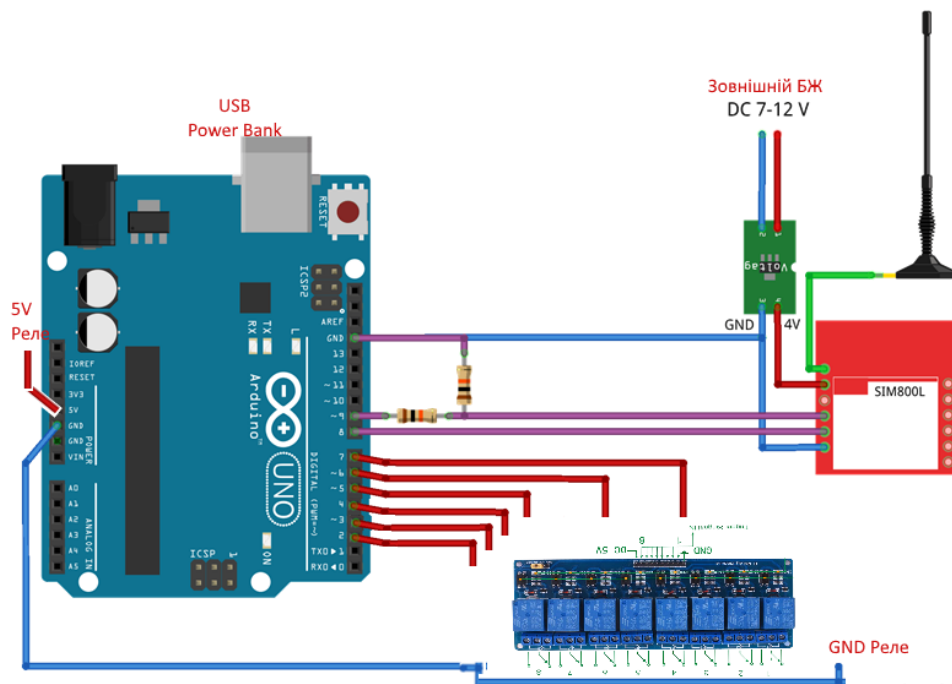


Рис. 1. Схема підключення компонентів.

Для передачі команд від користувача до системи віддаленого керування використовуються DTMF (Dual Tone Multi-Frequency) сигнали [5], які є стандартом для тонального набору в телефонних мережах. DTMF дозволяє передавати інформацію про натиснуті клавіші за допомогою комбінацій звукових частот, що значно підвищує швидкість та надійність передачі команд порівняно з імпульсним набором. Система розроблена таким чином, щоб розпізнавати вхідні DTMF сигнали, отримані через GSM модуль, та виконувати відповідні дії, наприклад, вмикання або вимикання підключених електроприладів. Такий підхід забезпечує зручність управління системою, оскільки користувач може відправляти команди з будь-якого місця, де є сигнал мобільного телефону, використовуючи стандартну клавіатуру телефону або мобільного додатку.

Література

1. Петли В. А. Проекты с использованием контроллера Arduino. – 2-е изд. перераб. и доп. – СПб.: БХВ-Петербург. 2015.
2. SIM800L Design Datasheet PDF. (GSM/GPRS Module) Hardware Design. URL: <https://datasheetpdf.com/datasheet/SIM800L.html> (дата звернення 05.05.2023).
3. Порівняння характеристик модулів SIMCom 800. URL: https://greenhouse.cv.ua/wp-content/uploads/2021/11/SIM800_compartion-1-scaled.jpg.
4. SIM800 Series_AT Command Manual_V1.10. URL: <http://codius.ru/file/download/4f7cb937-b8a7-4e28-bd24-c23d9a03c9da> (дата звернення 05.05.2023).
5. Бузов Є.В. Митник М.М. Комп'ютерні мережі. Підручник. Том 2. – Львів, «Магнолія 2006», 2020. – 204 с.

Секція 2. Мережні, оптоволоконні технології та безпека

УДК 621.382

ПРОБЛЕМИ АНАЛІЗУ ТРАФІКУ В МЕРЕЖІ ІОТ З ТЕХНОЛОГІЄЮ LI-FI

¹Бушинський Д.А., ²Романов А.О.

¹*Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна*

²*Національний Авіаційний Університет*

E-mail: dbushynskiy2002@gmail.com, anton3329@gmail.com

CHALLENGES OF TRAFFIC ANALYSIS IN IOT NETWORK WITH LI-FI TECHNOLOGY

Suggestions for improving the security of the interaction of Internet of Things and Li-Fi technologies by classifying and analyzing network traffic.

Сучасні комунікаційні системи та мережі інтернету речей продовжують зростати, знаходячи застосування у всіх сферах людської діяльності. Ідея ІоТ значно покращила якість сучасного життя ці рішення суттєво змінили перспективи технологій. Задіяно різні галузі, включаючи промисловість, охорону здоров'я, будинки, автомобільну промисловість, спорт, розваги та багато інших. Це досягається завдяки широкомасштабному розгортанню сенсорних вузлів або Sensor Nodes (SN) або інтелектуальних пристроїв із можливістю вимірювання та звітування [4]. Однак це залучення викликає серйозні проблеми, оскільки через мережу потрібно пройти багато трафіку. Таким чином, різні класи мережевого трафіку; наприклад, ті, що генеруються за допомогою голосу, фінансових транзакцій, безпілотних автомобілів, SN та інших, є критичними для відповідних секторів і потребують швидкого проходження або фільтрації через проблеми безпеки. Розвиток ІоТ призводить до експоненціального збільшення розумних пристроїв і датчиків які генерують величезну та різномірну кількість мережевих даних. Таким чином, вимоги до різних додатків в інтернеті речей швидко зростають, що призводить до попиту на більш точну класифікацію мережевого трафіку.

Пристрої потребують швидшої, безпечної та енергоефективної передачі даних. Зокрема, ми бачимо зростаючу потребу в гарантованій пропускній здатності з низькою затримкою в поєднанні з позиціонуванням не лише в повсякденному житті, доповненій реальності, але й у контролі промислових процесів у реальному часі. Комунікаційні та мережеві технології Li-Fi можуть надати ефективний і недорогий канал для повсюдного зв'язку в мережах ІоТ [2]. Він може забезпечити покращену швидкість передачі даних із низьким енергоспоживанням [7]. На відміну від радіочастотних хвиль, які використовуються Wi-Fi, світло не може проникати крізь стіни та двері. Це робить його більш безпечним і полегшує контроль, хто може підключатися

до мережі [1]. Очевидно, що майбутнє Інтернету речей значною мірою залежить від його взаємодії з технологією Light Fidelity.

Однак у таких системах традиційні методи керування мережею для моніторингу та аналізу даних стикаються з деякими проблемами, наприклад, з точністю та ефективною обробкою великих даних у режимі реального часу. Машинне навчання або Machine Learning (далі - ML) ефективно використовується для полегшення аналітики та виявлення аномалії у системах великих даних для розпізнавання прихованих і складних закономірностей. Дослідники в області мереж застосовують моделі ML для програм моніторингу та аналізу мережевого трафіку або Network Traffic Monitoring and Analysis (NTMA), наприклад, класифікації та прогнозування трафіку.

Застосування ML в NTMA забезпечує підвищення якості функціонування та безпеки мереж IoT. Регулярний моніторинг трафіку, створеного з систем IoT, важливий для їх належного функціонування та виявлення шкідливих дій [5]. Одним із таких видів діяльності є класифікація пристроїв IoT у мережевому трафіку [3]. Це дозволяє адміністратору відстежувати діяльність девайсів, що може бути корисним для належної реалізації якості обслуговування, виявлення шкідливих пристроїв тощо.

Для забезпечення належного контролю мережевого трафіку, дослідимо чотири ключові завдання в NTMA, зображені на рис. 1:

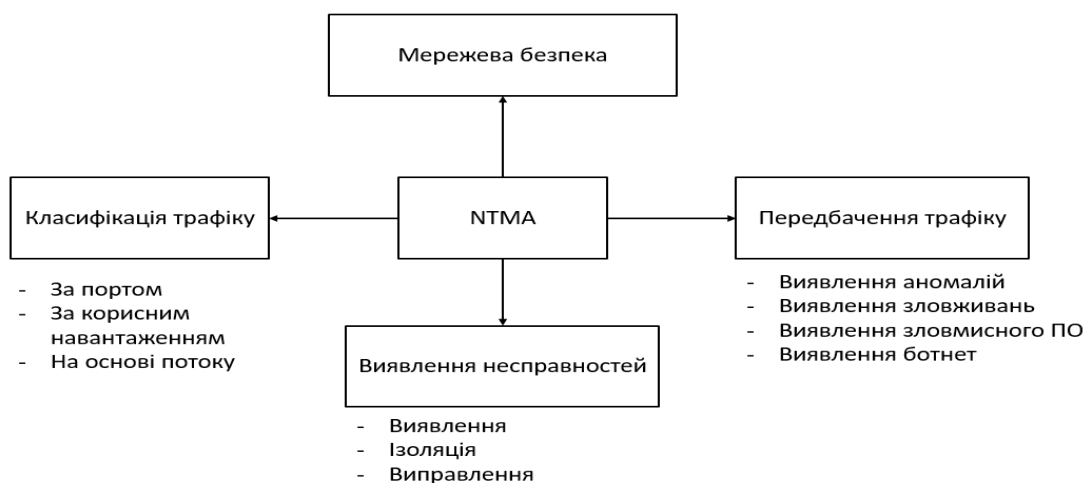


Рис. 1. Ключові завдання NTMA.

Методи машинного навчання, особливо алгоритми глибокого навчання або Deep Learning (DL), є одними з найпопулярніших методів обробки даних мережевого трафіку. Це пояснюється тим фактом, що сучасні комунікаційні системи та мережі IoT, мають відмінні характеристики, які відповідають алгоритмам DL. Ці особливості включають генерацію великих даних, складність, масштабність, зростаючу кількість протоколів у таких мережах тощо. Аналітичний підхід до великих даних можна використовувати для керування даними NTMA на основі машинного навчання. Підхід великих даних можна використовувати для класифікації трафіку атак у програмно-конфігурованій мережах або *Software-defined Networking* (SDN). Контроллер

SDN забезпечить обслуговування трафіку відповідно до політики, яка встановлена оператором мережі. Прибравши площину управління з мережевого обладнання, контролер реалізує централізовану систему керування, спрощує автоматичне керування мережею [8].

Традиційні методи для NTMA мають свої проблеми, наприклад, вони є неточними або сильно залежить від людського фактору. На відміну від традиційних методів, методи на основі DL мають наступні переваги [3]:

- Моделі DL не потребують значних людських зусиль, можуть використовувати різні репрезентативні шари та ефективні алгоритми для вилучення аномалій із величезних обсягів даних трафіку без розробки функцій. Ця перевага моделей дуже ефективна для методів NTMA, оскільки більшість даних керування мережею є немаркованими або напівмаркованими.

- Алгоритми здатні працювати з часово-просторовими даними, фіксуючи пов'язані залежності. Більшість даних про керування мережею, зібраних як набори даних часових рядів, можна аналізувати моделями DL з високою точністю.

- Крім того, нові парадигми машинного навчання, напр. федеративне навчання в основному розроблено для розподіленого впровадження методів глибокого навчання. Впровадження моделей DL за допомогою нових парадигм ML дозволяє навчати свою модель окремо на кожній машині.

Проведений аналіз проблем мережі IoT викликані великою кількістю генерованого трафіку. Окреслено способи контролю мережевих даних за допомогою NTMA. Досліджено впровадження машинного навчання для підвищення безпеки використання технології Li-Fi в мережах інтернет речей.

Література

1. Petrosino A., Striccoli, D., Romanov, O., Boggia, G., Grieco, L.A. Light Fidelity for Internet of Things: A survey. //Optical Switching and Networking// 2023, 48, 100732, <https://www.sciencedirect.com/science/article/abs/pii/S1573427723000036>
2. Enabled by Li-Fi Technology [Електронний ресурс] / S. P. Nazir, T. Mohammad, M. Ahmad: https://www.researchgate.net/publication/337388262_IoT_Enabled_by_Li-Fi_Technology.
3. Deep learning for Network Traffic Monitoring and Analysis / A. Shahraki, A. Mahmoud https://www.researchgate.net/publication/349056451_Deep_learning_for_Network_Traffic_Monitoring_and_Analysis_NTMA_A_survey.
4. The rise of traffic classification in IoT networks [Електронний ресурс] / Hamid Tahaei: <https://www.sciencedirect.com/science/article/abs/pii/S1084804520300126>.
5. IoT Network Traffic Classification Using Machine Learning Algorithms [Електронний ресурс] / K. Rakesh, S. Mayank: <https://ieeexplore.ieee.org/abstract/document/9590566>.
6. Toward Designing a Li-Fi-Based Hierarchical IoT Architecture [Електронний ресурс] / L. Albraheem, A. Aljaser – Режим доступу до ресурсу: <https://ieeexplore.ieee.org/abstract/document/8413064>.
7. Enhancing LiFi for next-generation Internet of things [Електронний ресурс] / J. Linnartz, E. Cunha – Доступу до ресурсу: <https://link.springer.com/article/10.1186/s13638-022-02168-6>.
8. Романов О.І., Свид І.В., Корнієнко Н.І., Романов А.О. Управління оптичною мережею контролером SDN на базі ONOS//Радіотехніка, № 210, 2022, С.184-192, DOI:10.30837/rt.2022.3.210.16.

РОЗПІЗНАВАННЯ ДЕФЕКТІВ НАМОТКИ ВОЛОКОННИХ КОТУШОК ВОГ

Іванов С.В., Олійник П.Б.

Навчально-науковий інститут телекомунікаційних систем

КПІ ім. Ігоря Сікорського, м. Київ, Україна

E-mail: poleinik@ukr.net; ivanov.sergiy@lll.kpi.ua

DETECTION OF FOG FIBER COIL WINDING DEFECTS

The algorithm for detection of fiber-optic gyro (FOG) fiber coil winding defects is presented and effectiveness of wavelet filtering for on-the-fly video processing during defect detection is estimated.

Точність волоконно-оптичного гіроскопа (ВОГ) суттєво залежить від якості намотки його чутливого елемента – котушки. В ідеалі намотана котушка не повинна мати дефектів намотки, і волокно повинно утворювати періодичну однорідну структуру. Типові дефекти намотки – пропуск витка та набіг витка на раніше намотані витки цього ж шару – показано на рис. 1.



Рис.1. Типові дефекти намотки: а – пропуск витка, б – набіг на витки

Аналогічну до рис. 1б картину (виток поверх інших, що утворює порушення структури) дають пристіночні дефекти намотки, викликані тим, що волокно не вміщується між стінкою каркасу котушки і передостаннім витком в шарі. При намотці котушок ВОГ за допомогою верстата [1] доцільно застосувати автоматизований контроль якості на основі використання машинного зору.

Для використання машинного зору перш за все треба забезпечити високу якість зображення з камери. Для цього запропоновано використати, крім класичного гаусівського згладжування, вейвлет-фільтрацію [2, 3], однак треба визначити ефективність застосування такої фільтрації в реальному часі.

Безпосередньо для розпізнавання дефектів намотки застосовуються три описаних нижче способи: аналіз контуру профілю намотки, аналіз відеопотоку з камери машинного зору за різницею між кадрами та аналіз штучно створених відблисків волокна.

Автори [4] застосували аналізу профілю намотки в кожному кадрі шляхом запису та аналізу координат піків профілю намотки. Недоліком алгоритму є те, що він ніяк не враховує наявність фланців котушки, а також наявність зазорів між витками, що може призводити до хибних спрацювань.

Авторами [5] запропоновано алгоритм, що виявляє дефекти шляхом виявлення різниці між кадрами відео потоку, отриманого з камери, що знімає

профіль катушки. Далі знов-таки виділяються координати піків профілю волокна і по їх різниці визначається наявність дефектів. Недоліком такого алгоритму є необхідність точної синхронізації обертання намотуваної катушки ВОГ та моментів зйомки кадрів камерою машинного зору для виявлення різниці між профілем намотки в однакових кутових положеннях катушки.

В [6] застосовано освітлення, яке створює відблиски на волокні на темному фоні, і наявність дефектів можна визначати за центрами цих відблисків. Недоліком є прискорене зношення камери і складність забезпечення освітлення, яке дає відблиски від волокна в області, близькій до профілю намотки, і форму відблисків, близьку до круга. Крім того, для роботи такого способу виявлення дефектів, необхідна зміна системи освітлення залежно від відбиваючої здатності волокна для створення близьких умов роботи алгоритму.

Метою дослідження є розробка алгоритму розпізнавання дефектів намотки катушок ВОГ та оцінка ефективності використання вейвлет-фільтрації в реальному часі при обробці зображення з камери машинного зору.

Для оцінки якості вейвлет-фільтрації було проведено фільтрацію зображення з камери такими вейвлетами: Хаара; Добеші 2 і Добеші 4; Симмлетом 2 і 4; Койфлетом 1 і 4; Біортогональними фільтрами 1.3 та 3.5.

Як міру якості фільтрації використано середньоквадратичну похибку RMSE (середньоквадратичне значення різниці між відфільтрованим зображенням і вихідним зображенням, до якого було додано шуми):

$$RMSE = \sqrt{\frac{1}{M \cdot N} \sum_{i=1}^M \sum_{j=1}^N (I_{i,j} - A_{i,j})^2} \quad (1)$$

де M , N – ширина і висота зображення, I – значення інтенсивності пікселя вихідного зображення, A – значення інтенсивності пікселя фільтрованого зображення; i, j – індекси підсумовування. Чим менше значення такої різниці, тим менше шумів у зображенні.

В таблиці 1 наведено оцінку якості фільтрації зображення з камери (рис.2) з переліченими вище вейвлетами; в третій колонці для наочності наведено різницю RMSE зображення рис. 2 і фільтрованого зображення.

Найбільш ефективними виявилися вейвлети Хаара і Симмлет 2.

Таблиця 1. Оцінка якості фільтрації зображення.

Зображення	RMSE зображення	Різниця RMSE
Зашумлене гаусовим шумом (рис.2.)	0,005582	-
Фільтрація вейвлетом Хаара (haar)	0.003019	0.002563
Фільтрація вейвлетом Добеші 2 (db2)	0.003173	0.002409
Фільтрація вейвлетом Добеші 4 (db4)	0.003305	0.002276
Фільтрація Симмлетом 2 (sym2)	0.003021	0.002561
Фільтрація Симмлетом 4 (sym4)	0.003295	0.002286
Фільтрація Койфлетом 1 (coif1)	0.003176	0.002406
Фільтрація Койфлетом 2 (coif2)	0.003404	0.002178
Біортогональним фільтром 1.3 (bior1.3)	0.003198	0.002384
Біортогональним фільтром 3.5 (bior 3.5)	0.003313	0.002269

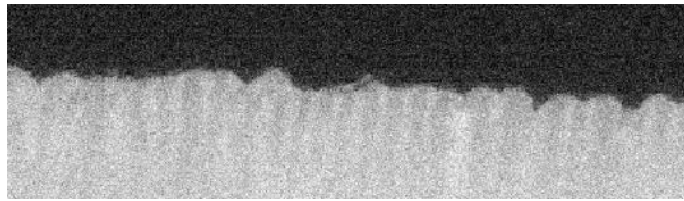


Рис.2. Зображення з камери з гаусовим шумом.

В основу розробленого авторами алгоритму покладено ту ж ідею, що і в публікації [4] – виділення профілю намотки, і подальший його аналіз.

Основні кроки роботи запропонованого авторами алгоритму такі:

- зображення перетворюється в градації сірого – тобто з пікселів буде вилучено інформацію щодо тону та насиченості, а залишаться лише значення яскравості, після чого згладжується гаусовим фільтром 5x5 або, опціонально – вейвлетами;

- проводиться бінарізація за алгоритмом Оцу, що дозволяє розділити пікселі зображення на два класи ("корисні" та "фонові"), за рахунок нескладного статистичного аналізу зображення, який при розділенні пікселів на класи робить так, щоб дисперсія всередині одного класу була мінімальною [7];

- для топологічного аналізу оцифрованих бінарних зображень використано алгоритм відстеження меж, який дозволив виділити контури [8];

- серед виділених контурів вибираються контури з довжиною не менше 100 пікселів (відсівання шумів).

Кожен вибраний контур горизонтується для спрощення аналізу даних. Після цього проводиться виділення локальних максимумів і мінімумів контуру, розпізнаються за зміною координат і відкидаються частини зображення, що відповідають фланцям котушки, і дрібні зміни висоти профілю намотки. Наявність дефекту «пропуск витка» визначається за відстанню по осі абсцис між сусідніми максимумами (більше діаметра волокна + зазор між витками), а «набіг волокна поверх шару» - за зміною вертикальної відстані між сусідніми екстремумами (більше за 2/3 діаметра волокна).

За наявності дефектів намотки вони виділяються на кадрі і про це повідомляється керуюча програма автоматичної станції намотки. Приклад зображення з виділеними дефектами наведено на рис. 3.

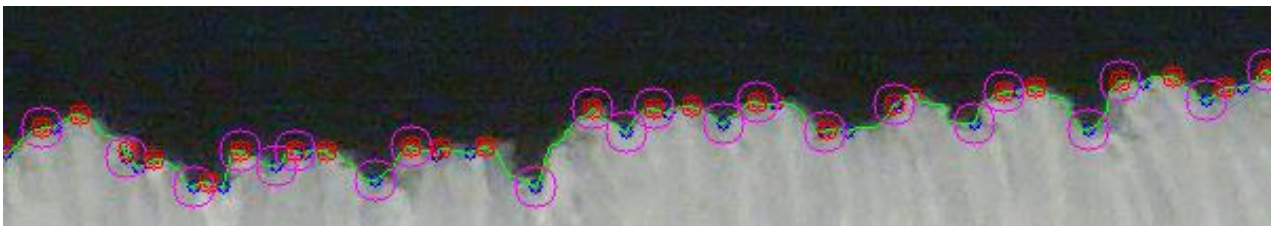


Рис.3. Зображення з камери з виділеними дефектами.

На рисунку виділено визначені максимуми і мінімуми профілю намотки (червоними і синіми колами маленького діаметру) та дефекти (фіолетовими

колами великого діаметру). Оскільки котушка намотана «внавал», вона містить багато дефектів, включаючи пропуски та перескоки витків.

Як показав експеримент, при номінальній частоті кадрів камери 30 кадрів/с, реальна частота обробки кадрів при виявленні дефектів складає 29,6..29,9 кадрів/с без застосування вейвлет-фільтрації і 12,6..14.5 кадрів/с при її застосуванні. Таким чином, застосування вейвлет-фільтрації недоцільне при виконанні намотки зі швидкістю 2 витки/с і більше, оскільки на один виток буде реєструватися менше 5 кадрів.

Висновки. Запропонований алгоритм може бути застосований для виділення розпізнавання дефектів намотки катушок ВОГ, причому застосування вейвлет-фільтрації при виконанні намотки зі швидкістю 2 витки/с і більше недоцільне.

Література

1. Іванов С. В., Олійник, П. Б., & Вірченко, Г. А. (2023). Намоточна машина для виготовлення катушок волоконно-оптичних гіроскопів. Збірник матеріалів Міжнародної науково-технічної конференції «ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ», 112–116. <http://conferenc.its.kpi.ua/proc/article/view/281185>
2. Капшій О.В. Вейвлет-перетворення у компресії та попередній обробці зображень. / О.В. Капшій, О.І. Коваль, Б.П. Русин – НАНУ, Фіз.-мех. ін.-т ім. Г. В. Карпенка.– Львів: Сполом, 2008.– 208 с.
3. Vyas, Aparna Review of the Application of Wavelet Theory to Image Processing /Aparna Vyas, Joonki Paik // IEIE Transactions on Smart Processing and Computing. – 2016. – Vol. 5, no. 6. – pp. 403 – 417. – DOI: <https://doi.org/10.5573/IEIESPC.2016.5.6.403>
4. Капшій О.В. Вейвлет-перетворення у компресії та попередній обробці зображень. / О.В. Капшій, О.І. Коваль, Б.П. Русин – НАНУ, Фіз.-мех. ін.-т ім. Г. В. Карпенка.– Львів: Сполом, 2008.– 208 с.
5. Vyas, Aparna Review of the Application of Wavelet Theory to Image Processing /Aparna Vyas, Joonki Paik // IEIE Transactions on Smart Processing and Computing. – 2016. – Vol. 5, no. 6. – pp. 403 – 417. – DOI: <https://doi.org/10.5573/IEIESPC.2016.5.6.403>
6. 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. – DOI: [https://doi.org/10.1016/S0736-5845\(00\)00030-2](https://doi.org/10.1016/S0736-5845(00)00030-2)
7. Vala, Hetal J. A review on Otsu image segmentation algorithm / Hetal J. Vala, Astha Baxi // International Journal of Advanced Research in Computer Engineering & Technology (IJARCET). – 2013. – Vol. 2 (2).– p.387.
8. Suzuki, Satoshi Topological structural analysis of digitized binary images by border following / Satoshi Suzuki, Keiichi Abe // Compute Vision, Graphics and Image Processing. – 1985. – Vol. 30, Issue 1. – pp. 32 – 46. – DOI: [https://doi.org/10.1016/0734-189X\(85\)90016-7](https://doi.org/10.1016/0734-189X(85)90016-7)

MICROSTRIP 4-RESONATOR FILTERS WITH ATTENUATION POLES

Galitskiy I., Kamarali R., Shevtsov K., Kirilyuk V.

*National Technical University of Ukraine “
Igor Sikorsky Kyiv Polytechnic Institute”*

Educational and Research Institute of Telecommunication systems

*E-mail: ilyagal26@ukr.net, r.kamarali@kpi.ua,
shewtsov.kostya@gmail.com, kuruvall1999@gmail.com*

МІКРОСМУЖКОВІ 4-РЕЗОНАТОРНІ ФІЛЬТРИ З ПОЛЮСАМИ ЗАГАСАННЯ

У статті наводяться результати моделювання чотирьохрезонаторних фільтрів методами електродинаміки та теорії кіл.

The article presents the results of modeling four-resonator filters using the electrodynamic method and bridge circuits.

Resonators can be implemented using a variety of technologies, including microstrip lines, which are popular due to their planar structure and ease of integration with printed circuit boards [1]. These filters can also be reproduced on focused elements.

The filter pictured below was modeled by CST Studio Suite. Dielectric permeability $\epsilon=2.8$, substrate thickness – 2 mm, strip thickness – 5.3 mm, $\tan\delta=0.001$.

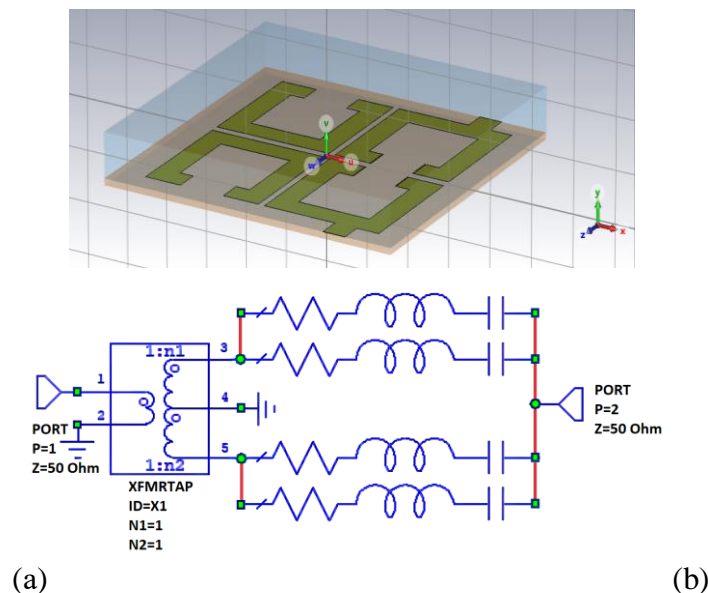


Fig. 1. (a) Topology of the CST Studio Suite four-resonator filter. (b) AWR equivalent circuit.

In fig. 2 (a) the gain of S_{21} where Fano resonance has formed, exhibiting anomalously high attenuation of about -45dB and -30dB at the peaks and a narrow

resonant characteristic around $f = 0.82$ GHz.

Metamaterials are usually diagrams of equivalent chain models. Figure 1 (b) shows the equivalent circuit modeled in the AWR Microwave Office software. In this case, a series RLC circuit is connected to the two arms of the transformer [2]. The simulation helped to build a microstrip filter not only with microstrips, but also with a bridge filter circuit. Figure 2 shows the result of the scheme. Bandwidth from 780 to 860 MHz. Attenuation is up to -40dB at peaks. The poles are formed because there are two paths of energy propagation that "intervene" in the region of zero transmission and create a "quasi-trapped" mode or "trapped" mode [3].

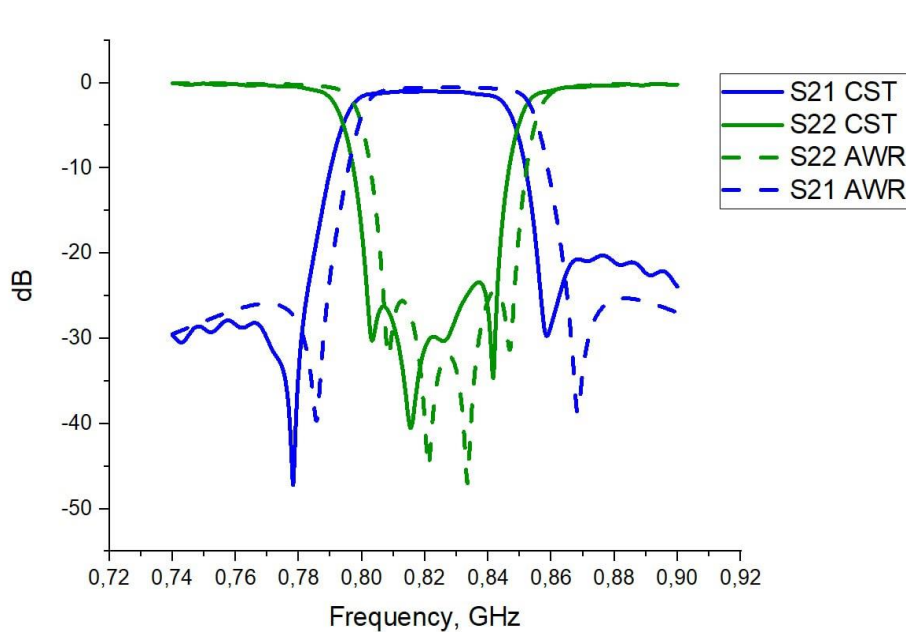


Fig. 2. Characteristic of the four-resonator filter in CST Studio Suite and AWR.

After studying the obtained results, we can come to the conclusion that the reflection coefficient does not change sharply in the regions of the poles. Therefore, a sharp decrease in the transmission coefficient can be explained only by the fact that trapped modes appear inside the structure in the region of such frequencies. The energy of these modes is not radiated outward, but "circulates" along the closed path 1-2-3-4-1, as shown in Fig. 3. Such poles can be reached with the help of additional connections between resonators, which makes it possible to create conditions for the formation and maintenance of these trapped modes.

The introduction of additional connections between resonators not only contributes to the formation of trapped modes, but also allows to control their properties.

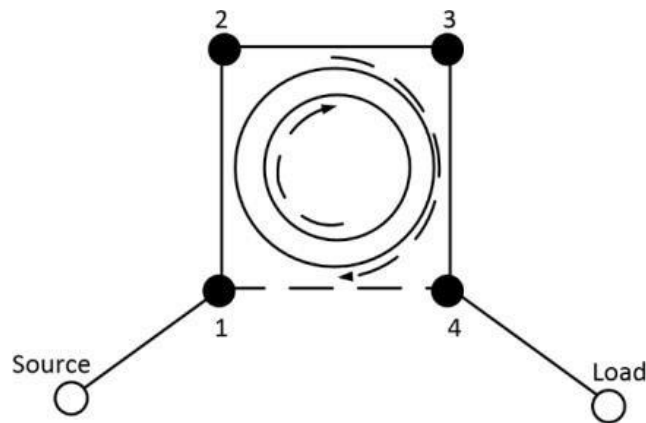


Fig. 3. Trajectory of propagation of trapped modes in a four-resonator filter.

By changing the characteristics of these connections, it is possible to change the frequency characteristics of the trapped modes, which opens up wide opportunities for adjusting the properties of the structure. Thus, the study of the interaction between resonators and their influence on the formation of trapped modes is key to the development of new devices with improved characteristics [4].

Conclusion. Therefore, trapped modes appear in the form of extinction poles (interference of even and odd oscillations). A sign of this is the presence of two independent energy paths along which interfering oscillations propagate. With correctly selected parameters (resonator coupling coefficients, resonance frequencies) at a certain frequency, a complete exchange of resonator energies occurs in the direction perpendicular to the direction of energy propagation from the input to the output.

All 3 modeling methods gave a similar, even almost identical result, which testifies to the variety of variations in the performance of the investigated filters.

Acknowledgement. This work was supported by NATO SPS G6002 “3D metamaterials for energy harvesting and electromagnetic sensing”.

References

1. USSR Inventor's Certificate 1529321.
2. Ільченко М. Й., Живков О. П., Камаралі Р. В. та ін. "Моделювання електромагнітно індукованої прозорості за допомогою RLC-схем і метаматеріальної комірки". Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».
3. Zhivkov, O., Stoianov, I., Tychynskiy-Martyniuk, V., Galitskiy, I., Shevtsov, K., & Kamarali, R. (2023). Modeling of Microwave and Terahertz Trapped Modes by Circuit Theory Methods. 2023 IEEE 6th International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2023. Presented at the 6th IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2023, Kyiv, Ukraine, Nov 13 2023 - Nov 18 2023. <https://doi.org/10.1109/UkrMiCo61577.2023.10380329>.
4. Cameron, R. J., Kudsia, C. M., & Mansour, R. R. (2018). Microwave Filters for Communication Systems. doi:10.1002/9781119292371.

ПЕРЕВАГИ ТА НЕДОЛІКИ ВИКОРИСТАННЯ МІКРОСЕРВІСНОГО ПАТТЕРНУ ПРОЕКТУВАННЯ

Маньківський В.Б., Коршак О.О.

Навчально-науковий інститут телекомунікаційних систем

КПІ ім. Ігоря Сікорського, Україна

E-mail: v.b.mankivskiy@gmail.com , korshak1234@gmail.com

ADVANTAGES AND DISADVANTAGES OF USING THE MICROSERVICE DESIGN PATTERN

The paper discusses the rationale and benefits of microservice architecture, including modularity, flexibility, scalability, and error isolation. Advantages such as rapid development, easy technology replacement, and speed of innovation are described. The disadvantages, such as system complexity, distributedness and testing issues, are highlighted.

У роботі розглянуто обґрунтування та переваги мікросервісної архітектури, включаючи модульність, гнучкість, масштабованість та ізоляцію помилок. Описано переваги, такі як швидка розробка, легка заміна технологій та швидкість інновацій. Висвітлені недоліки, як складність системи, проблеми розподіленості та тестування.

Обґрунтування вибору мікросервісної архітектури. Модульність і розділення функціональності: Мікросервісна архітектура дозволяє розділити великі програми на невеликі, незалежні сервіси. Це полегшує розробку, тестування і підтримку системи, оскільки кожен сервіс може бути розроблений, тестований і оновлюваний окремо.

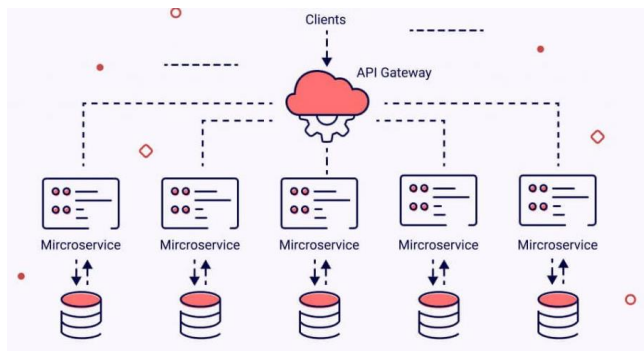
Гнучкість і масштабованість: Мікросервісна архітектура дозволяє гнучко масштабувати окремі сервіси залежно від їхньої навантаженості та вимог. Це дозволяє оптимізувати використання обчислювальних ресурсів та забезпечує більшу ефективність системи.

Ізоляція помилок: У мікросервісній архітектурі помилки у одному сервісі не впливають на решту системи, оскільки кожен сервіс працює незалежно. Це підвищує надійність та стійкість системи до збоїв.

Прискорена розробка та розгортання: Розробка окремих мікросервісів може проводитися паралельно різними командами, що сприяє швидкій розробці та впровадженню нового функціоналу.

Легка заміна технологій: Вибір мікросервісної архітектури робить систему менш залежною від конкретних технологій. Кожен сервіс може використовувати технології, що найкраще підходять для його завдань.

Підтримка розподіленого розгортання: Мікросервіси добре підходять для розподіленого розгортання на різних серверах або хмарних.



сунук 1. Microservice architecture.

На Рис.1 показана типова мікросервісна архітектура з окремим виділенням БД для кожного сервісу [1]. В даній архітектурі використаний паттерн API-gateway, який розподіляє всі запити до відповідного сервісу.

При цьому, явно виділяється недолік такого підходу в тому, що є одна точка виходу із строю, а також централізований підхід до керування.

Окрім того, API-gateway вионує додаткові функції: логування, трасування, аутентифікацію. Дані додаткові функції підвищують гнучкість такої системи.

Переваги та недоліки мікросервісної архітектури. Мікросервісна архітектура визначається сукупністю властивостей, які сприяють ефективному масштабуванню застосунків як у горизонтальному, так і у вертикальному напрямках. Крім того, ці властивості сприяють створенню надійних та відмовостійких застосунків [2].

Масштабованість: Однією з ключових переваг мікросервісної архітектури є її здатність ефективно масштабуватися як горизонтально, так і вертикально. Це робить процес розробки та розгортання економічно більш вигідним і менш часозатратним, особливо у порівнянні з монолітними архітектурами. У монолітних системах зазвичай єдиним методом масштабування є копіювання всієї програми, навіть якщо потрібно збільшити обсяг лише певних модулів [3]. Це стає особливо актуальним, коли збільшується кількість користувачів застосунку.

Відмовостійкість: У мікросервісних застосунках, завдяки їхній низькій зв'язності, виявляється природна властивість відмовостійкості. Це означає, що у випадку, якщо певний модуль системи припиняє свою роботу, його можна легко вимкнути, замінити або відлагодити, не призводячи до зупинки роботи всієї системи в цілому.

Технологічність: Кожен індивідуальний мікросервіс у системі може мати свій власний технологічний стек. Крім того, цей стек можна легко оновлювати. Неможливо враховувати всі аспекти від кожного мікросервісу, можливість все ще значно ширші порівняно з монолітним застосунком.

Простота у розумінні окремого мікросервісу: Кожен окремий мікросервіс є меншим за розміром, ніж повноцінний монолітний застосунок. Одночасно код в межах мікросервісу має високий рівень пов'язаності, і так, оскільки система має низьку зв'язність, кодова база є набагато простішою.

Незважаючи на велику кількість сильних сторін, мікросервісні застосунки також мають свої слабкі сторони [4]. Деякі з цих недоліків не є проблемою в монолітних застосунках, що підкреслює важливість правильного використання та реалізації для кожної:

- Складність системи в цілому: Кожен окремий мікросервіс може бути досить зрозумілим, проте при розгляданні системи в цілому вся

мікросервісна архітектура стає досить складною та значною важчою для розуміння, ніж монолітна.

- Розподіленість: Мікросервісна архітектура побудована на ідеї незалежності мікросервісів. Основною складністю є саме взаємодія цих мікросервісів та використання досить складних протоколів спілкування.

- Відлагодження: З урахуванням вищезгаданих проблем можна додати, що відлагодження системи в цілому є складнішою задачею.

Висновок. Мікросервісна архітектура є потужним інструментом для розробки сучасних програмних систем. Обґрунтовано вибір цієї архітектури з точки зору модульності, гнучкості, масштабованості, ізоляції помилок, швидкості розробки та розгортання, легкої заміни технологій, швидкості інновацій та підтримки розподіленого розгортання [5]. Вона сприяє підвищенню ефективності, надійності і стійкості програмних систем, а також полегшує їхнє розвиток і супровід. Проте, разом з численними перевагами, мікросервісна архітектура має і свої недоліки. Складність системи, проблеми розподіленості, складнощі у тестуванні та відлагодженні можуть стати серйозними викликами для розробників. Однак правильне планування, проектування і впровадження можуть допомогти подолати ці проблеми і максимізувати переваги .

Література

1. Приходченко, С. Д., Роина, К. С., Поштак, Р. В. (2018). Обґрунтування вибору мікросервісної архітектури в порівнянні з монолітною. [Електронний ресурс]. URL: <http://ir.nmu.org.ua/handle/123456789/153837>
2. Новак, В. В. (2022). Порівняння монолітної та мікросервісної архітектур на прикладі корпоративного застосунку. [Електронний ресурс]. URL: <https://dspace.znu.edu.ua/jspui/handle/12345/9531>
3. Степанова, Н. І. (2022). АНАЛІЗ МІКРОСЕРВІСНИХ ТА МОНОЛІТНИХ АРХІТЕКТУР. Міжнародний науковий комітет, 91. [Електронний ресурс]. URL: https://www.dnu.dp.ua/docs/ndc/2022/materiali/25_%D0%9C%D0%9F%D0%97%D0%86%D0%A1-2022-1.pdf#page=91
4. Newman, S. (2019). Monolith to microservices: evolutionary patterns to transform your monolith. O'Reilly Media. [Електронний ресурс]. URL: https://books.google.com.ua/books?hl=uk&lr=&id=nNa_DwAAQBAJ&oi=fnd&pg=PP1&dq=Monolith+to+microservices:+evolutionary+patterns+to+transform+your+monolith.+O%27Reilly+Media&ots=eiUW1wn efH&sig=DNeWizndCLJrTox2-7RSz6OgYj4&redir_esc=y#v=onepage&q=Monolith%20to%20microservices%3A%20evolutionary%20patterns%20to%20transform%20your%20monolith.%20O'Reilly%20Media&f=false
5. Thönes, J. (2015). Microservices. IEEE software, 32(1), 116-116. [Електронний ресурс]. URL: <https://ieeexplore.ieee.org/abstract/document/7030212>

ПІДВИЩЕННЯ ЯКОСТІ ОБСЛУГОВУВАННЯ В МЕДИЧНІЙ СФЕРІ ЗА РАХУНОК ВИКОРИСТАННЯ DOCKER ТА KUBERNETES

Кравченко М.А., Романов М.О.

*Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського,
Національний Авіаційний Університет, Україна
E-mail: mishakravchenk@gmail.com, mykppl@gmail.com*

DIRECTIONS FOR IMPROVING THE QUALITY OF SERVICE IN THE MEDICAL FIELD USING DOCKER AND KUBERNETES

Today, the world is experiencing a great leap in the amount of data on the Internet. This did not escape the medical field either. The main reason for this was the digitization of medical data. Because of this, the healthcare industry faces several challenges, such as management and storing large amounts of data, including electronic health records and laboratory test results, handling large and variable workloads, and processing and storing sensitive data. Docker and Kubernetes can help solve these problems.

Сьогодні світ переживає великий стрибок у збільшенні обсягу даних в інтернеті. Це не обійшло і медичну галузь. З метою підвищення якості обслуговування пацієнтів в медичній сфері, проводиться автоматизація і цифровізація обробки медичних даних (рис.1). Через це галузь охорони здоров'я стикається з кількома проблемами, таких як керування та зберігання великих обсягів даних пацієнтів, включаючи електронні медичні записи та результати лабораторних досліджень, робота з великими та змінними навантаженнями, обробки та зберігання конфіденційних даних пацієнтів. Вирішити ці проблеми може допомогти Docker та Kubernetes [1, 2].

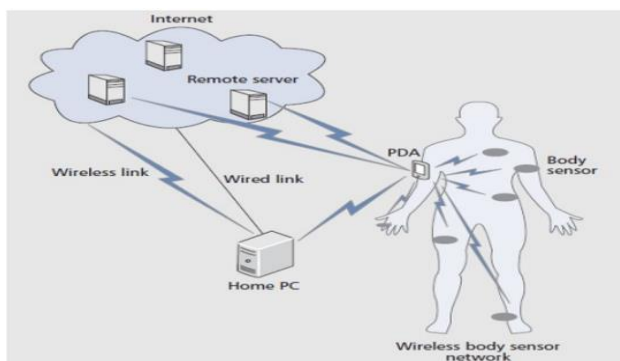


Рис.1. Приклад впровадження цифровізації в галузі охорони здоров'я.

Припустимо, що ви розробили велику програму, для роботи якої необхідні декілька залежностей, і запустили її на Linux. Тепер нам необхідно якось скопіювати все те, що потрібно для однакової роботи програми будь де. Перше що може прийти в голову це використання віртуальних машин. Для неї ми можемо установити потрібну операційну систему, залежності,

запустити нашу програму і все буде працювати. Але в сучасних реаліях, де всі люблять розпилувати одну велику програму на декілька маленьких і

називати це мікро сервісною архітектурою, такий підхід буде не дуже оптимальний [3, 4]. Оскільки кожна віртуальна машина запускає різні ОС, це все буде працювати не дуже швидко. До цього всього іноді нам треба запускати декілька копій одного і того ж сервісу, тому навантаження буде тільки рости. Всі ці проблеми можна вирішити, використавши технологію контейнеризації [5, 6].

Контейнеризація дозволяє об'єднати програмне забезпечення разом із усіма його залежностями в окремий контейнер, щоб його можна було запускати без проблемного процесу налаштування на будь якому комп'ютері де є встановлений Docker.

Робота Docker схожа на роботу віртуальної машини але є одна ключова різниця. З Docker ми позбуємося гіпервізора, а замість того щоб віртуалізувати "железо" комп'ютера, ми віртуалізуємо лише операційну систему, значить нам немає необхідності в окремих гостьових ОС, тому що контейнери використовують ядро того ОС сервера, де ми працюємо за допомогою додатку Docker Engine. Тому ми витрачаємо менше ресурсів при роботі з легковажними контейнерами. При цьому додатки залишаються все так же ізольовані від системи і інших додатків.

Тепер може виникнути питання про те, як запускати декілька контейнерів одночасно. В реальному додатку мікро сервісів може буди кілька десятків і всіма ними необхідно якось керувати, обновляти, виділяти ресурси, балансувати навантаження. Тут нам на допомогу приходить Kubernetes.

Kubernetes - це платформа з відкритим кодом для автоматизації розгортання, масштабування та керування контейнерними програмами. Він забезпечує інфраструктуру, орієнтовану на контейнери, що дозволяє розробникам легко й ефективно розгортати, масштабувати та керувати своїми програмами в різних середовищах. Kubernetes має кілька ключових функцій, які роблять його потужною платформою для керування контейнерними програмами, зокрема:

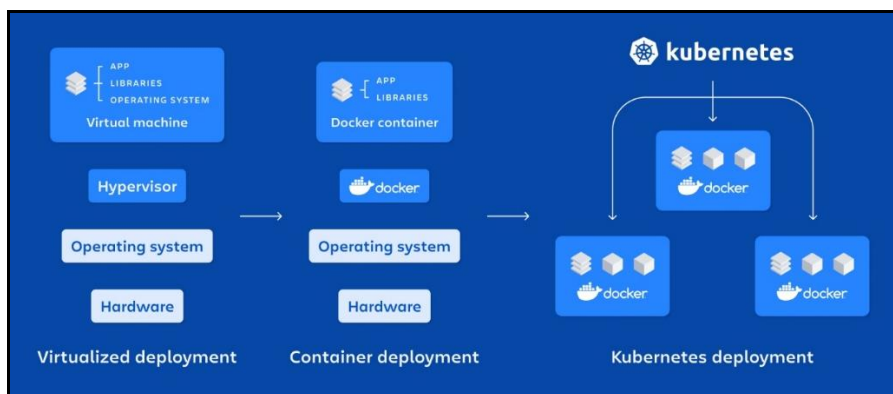


Рис.2. Порівняння використання віртуалізованого та контейнерного розгортання програм.

Масштабуванн
я кількості реплік
певної програми на
основі
використання ЦП
або пам'яті (рис.2).
Перезапуск
несправних
контейнерів.
Розподілення
вхідного

мережевого трафіку між кількома репліками. Kubernetes та Docker можуть допомогти організаціям охорони здоров'я кількома способами. Одним із ключових способів використанням контейнерів Docker в охороні здоров'я є розгортання систем електронних медичних записів (EHR). EHR необхідні для сучасної системи охорони здоров'я, але використовуючи лише традиційні віртуальні машини, їх може бути важко розгорнути та підтримувати, оскільки управління ресурсами, такими як CPU, пам'ять та мережа, виконується вручну адміністраторами, що може призвести до неоптимального використання ресурсів та складнощів у масштабуванні. Якщо раптово збільшиться обсяг даних, Kubernetes може автоматично розгорнути додаткові екземпляри програми для обробки навантаження. Наприклад, коли в лікарнях час пік, Kubernetes може підняти декілька екземплярів сервісу “базових функцій”, не чіпаючи інші сервіси. А після пікового навантаження, він відключить їх для економії ресурсів. Якщо один із сервісів перестане працювати, Kubernetes зможе швидко перезапустити його.

Kubernetes надає можливість налаштувати політики безпеки для контейнерів, такі як обмеження доступу до ресурсів, мережева ізоляція та контроль на рівні доступу. Також Kubernetes може інтегруватися з різними інструментами шифрування, які забезпечують захист конфіденційності даних. Наприклад, можна використовувати Kubernetes Secrets для зберігання та керування конфіденційними даними, які використовуються в контейнерах. Secrets дозволяють обробляти чутливі дані в межах файлу docker або коду додатка [2].

Kubernetes можна інтегрувати з іншими технологіями, такими як машинне навчання та Інтернет речей, що дозволить організаціям охорони здоров'я розробляти нові та інноваційні рішення для догляду за пацієнтами. Уявімо, що в лікарні використовується система моніторингу здоров'я пацієнта за допомогою смарт-браслетів, які вимірюють пульс, кількість пройдених кроків і їх рівень активності. Після того, як були зібрані і відправлені необхідні дані, Kubernetes починає їх оброблювати. Він відповідає за їх аналіз та інтерпретацію. Використання Kubernetes дозволяє легко масштабувати обробку даних в залежності від їх обсягу та обробляти велику кількість даних в реальному часі. Далі на основі аналізу даних, система генерує звіти про стан здоров'я пацієнта і надсилає дані медичному персоналу.

Docker дозволяє легко розгортати нові версії програмного забезпечення, а Kubernetes забезпечує автоматизоване керування оновленнями. Це дозволяє швидко внести зміни та виправити помилки у медичних системах.

Докер-контейнери також можуть бути корисними в дослідницькій частині охорони здоров'я. Вони забезпечують спосіб створення переносних і відтворюваних дослідницьких середовищ для аналізу даних і машинного навчання. Це дозволяє дослідникам легко ділитися своїми даними та методами з іншими та відтворювати отримані результати, що важливо для перевірки та розвитку попередніх досліджень. Припустимо, що дослідник займається аналізом геномних даних для виявлення генетичних мутацій, які можуть бути пов'язані з певними захворюваннями. Якщо він використовує Docker, то він може створити Docker образ, в якому запаковані необхідні бібліотеки та інструменти для обробки даних. Цим образом, він може ділитися з іншими науковцями та відтворювати аналітичне середовище на інших системах. Якщо обсяги даних будуть зростати, дослідник може використати Kubernetes для автоматичного масштабування обчислювальних ресурсів та запуску паралельних обчислень для швидкої обробки великих даних.

Підсумовуючи, контейнери Docker та Kubernetes— це потужні технології, які можна використовувати різними способами в галузі охорони здоров'я. Від програмного забезпечення в контейнерах до розгортання систем EHR, від відтворюваних досліджень до ізоляції конфіденційних даних пацієнтів, Docker-контейнери та Kubernetes надають низку переваг як постачальникам медичних послуг, дослідникам, так і пацієнтам.

Література

1. The Docker Handbook / Farhan Hasin Chowdhury / <https://www.freecodecamp.org/news/the-docker-handbook/#introduction-to-containerization-and-docker>
2. Romanov O., Nesterenko M., Mankivskyi B., Zhuk O. Principles of Building Modular Control Plane in Software-Defined Network/2023 |, DOI: [10.1007/978-3-031-16368-5_17](https://doi.org/10.1007/978-3-031-16368-5_17)
3. Basic Concepts in Cloud Native and Kubernetes / [Електронний ресурс] — Режим доступу: <https://www.healthtechzone.com/topics/healthcare/articles/2024/01/24/458477-basic-concepts-cloud-native-kubernetes.htm>
4. Benefits of Docker for the Healthcare Industry / Karan Singh / [Електронний ресурс] — Режим доступу: <https://collabnix.com/5-benefits-of-docker-for-the-healthcare-industry/>
5. Containerization in Healthcare / Jay Jayakumar / [Електронний ресурс] — Режим доступу: <https://jayjayakumar.medium.com/containerization-in-healthcare-bd0bd1525c3>
6. 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\
7. Романов О.І., Сколець С.С., Марінов А.І. Розгортання ONOS кластеру для емуляції роботи користувачької мережі SDN// Сімнадцята міжнародна НТК "Перспективи телекомунікацій", Київ, 2023 р., С 133-135.

ВНУТРІШНЄ ПОЗИЦІОНУВАННЯ ЗА ПОШУКОМ НАЙБЛИЖЧОГО ЗНАЧЕННЯ RSS ВИКОРИСТОВУЮЧИ ТЕХНОЛОГІЮ LI-FI

Романов О.І., Мікляєв Г.О.

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна
E-mail: a_i_romanov@ukr.net, glibmiklaiv@gmail.com*

INDOOR POSITIONING BY SEARCHING FOR THE NEAREST RSSI USING LI-FI TECHNOLOGY

The work analyzes the problems of positioning objects indoors. It is shown that the use of radio technologies to solve this type of problem results in a large error. Therefore, it is proposed to use technologies based on light waves. A method for solving the problem of positioning objects indoors is proposed. An algorithm is considered that allows solving the problem with fairly high accuracy.

Зараз відбувається четверта індустріальна революція і збільшення кількості інтернет речей (IoT). Є потреба в визначенні їх місцезнаходження для взаємодії між пристроями. Зовні та на великих місцевостях добре працює GPS, але всередині приміщень його функціонування не є достатньо необхідним. Як варіант рішення пропонується в цій статті використовувати позиціонування Li-Fi [1, 2]. Він може використовуватися для приміщень різних типів та для вирішення різних підзадач у позиціонуванні у **логістиці та управлінні запасами на складах** (оптимізація маршрутів, пошук товарів), **навігації всередині будівель, лікарні** (пошук медичного обладнання, керування руху лікарняних ліжок), тощо.

Для позиціонування в приміщеннях використовуються різні технології. Такі технології як Wi-Fi та Bluetooth, ZigBee, RFID є поширеними, і не потребують додаткового обладнання, при використанні вже як для передавання даних, але є досить неточні, також є обмеження на використання в чутливих місцях до радіопромінів, як лікарні, тощо. Такі технології як Ultra Wideband (UWB), чи за допомогою ультразвуку мають більшу точність, але потребують додаткового обладнання, що збільшує їх вартість. Також UWB потребує широкої радіосмути, що часто є недосяжним. Внутрішнє позиціонування на базі технології Li-Fi не використовує радіохвилі, що є перевагою в чутливих до радіовипромінення місцях. При наявності Li-Fi не потребує додаткового обладнання, та є точнішими за поширені технології у мікрохвильовому діапазоні [3].

В свою чергу, у Li-Fi є деякі обмеження, як сильний вплив завад від Сонця на прийнятну потужність, завада від відбитих променів, тощо.

Є різні методи визначення місцезнаходження. Як трилатерація, триангуляція, триангулатерація, на основі потужності від користувача (RSSI, Received signal strength indicator). Для триангуляції потрібно знати кути, а для трилатерації – відстані. Триангулатерації є комбінацією трилатерація та триангуляція, тому потрібно визначати і кути, і відстані. Оскільки найпростіше вирахувати та виміряти потужність, тому використано метод на базі RSSI. Модель такої системи, яка використовується для розрахунку, представлена на рис.1.

Є різні способи підрахунку місцезнаходження користувача залежно від інформації про стан каналу [4, 5]. Перевагою даного методу є не потреба в збереженні інформації і точність попередньо не задається. Недоліком є складність обчислень. Емпіричний обчислення потребує попереднього вимірювання потужності в кімнаті, але не потрібен математичний апарат. Цей метод оснований на пошуку найближчих попередньо обчислених значень (1). Для обчислення потрібні такі дані, як показник Ламберта (m), коефіцієнти підсилення (T для фільтра та $g(\theta)$ для оптичного концентратора), A – площа приймача, φ – кут передавача, θ кут приймача.

$$P_{rec} = P_{tr} \frac{(m+1)A}{2\pi d^2} \cos^m(\varphi) T g(\theta) \cos(\theta) \quad (1)$$

Алгоритм визначення місця знаходження користувача складається з двох частин: передрозрахунок для заданої моделі приміщення без користувачів та кінцевий розрахунок задля конкретної потужності сигналів користувача.

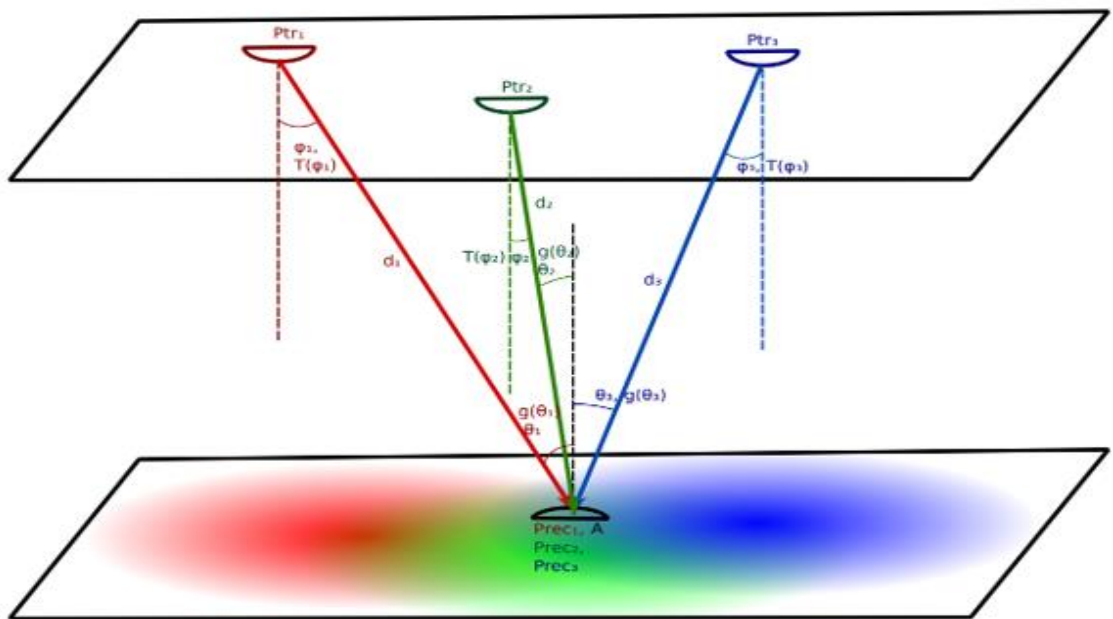


Рис.1

Загальний алгоритм виконання передрозрахунку наступний:

1. Ввід початкових параметрів системи, таких як місцезнаходження ламп, їх потужність, тощо.
2. Кімната фрагментується на квадрати заданої розмірності. Вважаємо, що на краю квадратів потужність рівна потужності її центру.
3. Розрахунок потужності в центрі кожного квадрату для кожної лампи використовуючи (1).
4. Збереження результатів обчислень. Наприклад в матриці із очікуваними значеннями потужності на підлозі від користувача (M_{row}). Матриця повинна бути трьох мірної: $X \times Y \times L$, де X та Y розташування обчислюваної точки за координатами x та y відповідно, а L номер лампи. Значення цієї матриці рівні потужності у відповідній точці підлоги від відповідної лампи.

Далі переходимо до розрахунку місцезнаходження користувача у динаміці його переміщення. Алгоритм рішення основної частини задачі наступний:

1. Користувач надсилає запит на визначення свого місцезнаходження в кімнаті та потужність прийнятого сигналу від кожної лампи P_{res} , масив $1 \times n$, де n кількість ламп.

2. Контролер обробляє інформацію надіслану користувачем (P_{res}) з урахуванням передобрахованих даних (M_{row}). Результатом є координати місцеположення користувача. Для цього:

I. Спочатку знаходить абсолютну різницю між матрицею розподілу потужностей по підлозі та потужністю від користувача ($M_{row}-P_{res}$, віднімання здійснюється відповідно до кожної лампи, але за кожною координатою). В результаті отримуємо трьохмірну матрицю різниць $M_{diff_{3d}}$, яка має ту саму розмірність як і M_{row} . Але її значення рівні абсолютній різниці між передобрахованим значенням і значенням отриманим користувачем.

II. Для знаходження координат знаходимо середньоквадратичне відхилення в центрі кожного квадрату підлоги кімнати загалом по всіх лампах. Для цього з матриці $M_{diff_{3d}}$, рахуємо середньоквадратичне значення за координатою L , для кожної координати X та Y . В результаті отримуємо матрицю $M_{diff_{2d}}$ з розмірністю $X \times Y$. Значення в кожній клітинці матриці є відхилення потужності користувача від приймача.

III. Чим менше значення відхилення, тим ближче показники вимірів потужності користувача до передобрахованого значення за даною координатою. Квадрат на підлозі, що відповідає клітинці матриці $M_{diff_{2d}}$ з найменшим значенням є найбільш вірогідним розташуванням користувача. Знаходимо цю координату.

3. Результат надсилає назад користувачу або обробляється системою.

Таким чином, запропонована технологія позиціонування об'єктів в середині приміщень. Розглянуто алгоритми, які використовуються у внутрішньому позиціонуванні, їх переваги та обмеження. Розглянуті методи та способи обрахунку для технології Li-Fi, переваги та обмеження. Проведено детальний опис алгоритму на базі RSSI, який складається на основі пошуку найближчого значення за передобрахунком. Проведено загальний опис реалізації алгоритму.

Література

1. Romanov, O., Dong, T.T., 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. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85085966325&partnerID=40&md5=abf8759d141835b8fcd8082fdb4b04dc>
2. Чумаченко К.Д., Романов О.І. Використання LI-FI в медицині // Сімнадцята міжнародна НТК "Перспективи телекомунікацій", Київ, 2023 р., С 119-121.
3. Romanov, O.I., Fediushyna, D.M., Dong, T.T. Model and method of Li-Fi network calculation with multipath light signals/(2018) 2018 International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2018. DOI: 10.1109/UkrMiCo43733.2018.9047550
- 4 Kaiyao Wang, Yongjun Liu, and Zhiyong Hong, "RSS-based visible light positioning based on channel state information," Opt. Express 30, 5683-5699 (2022)
- 5 Romanov, O.I., Hordashnyk, Y.S., Dong, T.T. Method for calculating the energy loss of a light signal in a telecommunication Li-Fi system/2nd International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2017 - 2017, 8095404, DOI: 10.1109/UkrMiCo.2017.8095404

НАДАННЯ ПОСЛУГ SIP-ТРАНКІНГ ЧЕРЕЗ ХМАРНІ SBC

Підпалій О.І., Нестеренко М.М.

*Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна*

E-mail: sashapispalyi@gmail.com; nikolaiy.nesterenko@gmail.com

У сучасних телекомунікаційних мережах технологія транкінгу протоколу ініціації сеансу через хмарні контролери стала необхідною для послуг голосового та відеозв'язку через мережі Інтернет-протоколу. Незважаючи на це, існують проблеми з продуктивністю та оптимізацією цих контролерів, особливо в умовах зростаючих обсягів даних та користувачів. Аналіз продуктивності хмарних контролерів дозволив зробити важливі аналітичні висновки, а розроблені стратегії оптимізації надали практичні рекомендації щодо покращення надання послуг хмарного транкінгу.

ENHANCING SIP TRUNKING SERVICE DELIVERY THROUGH CLOUD SBCS

In today's telecommunications networks, session initiation protocol trunking technology through cloud controllers has become necessary for voice and video communication services over Internet Protocol networks. Despite this, there are performance and optimization challenges for these controllers, especially in the face of growing data and user volumes. The performance analysis of cloud controllers revealed important analytical conclusions, and the developed optimization strategies provided practical recommendations for improving the provision of cloud trunking services.

Хмарні Session Border Controller (SBC) є ключовими елементами сучасних телекомунікаційних мереж [1], особливо в контексті надання послуг Session Initiation Protocol (SIP)-транкінгу через IP-мережі.

Хмарний SBC може виконувати наступні функції:

- контроль сесій;
- маршрутизація;
- забезпечення безпеки;
- транскодування;

Однак з постійним зростанням обсягів даних та кількості користувачів у мережах, хмарні SBC встають перед новими викликами та завданнями. Сучасні хмарні SBC є складними системами з великою кількістю налаштувань та можливостей [2].

Можна порівняти певні хмарні SBC за аналізом часу налаштування дзвінка, оцінкою якості дзвінка (MOS) та оцінкою використання ресурсів та масштабованості [3]. В якості прикладів слід використати такі хмарні SBC як Amazon Chime Voice Connector, Twilio Elastic SIP Trunking, Azure Communication Services, Dialogflow Telephony Gateway та Oracle Cloud Infrastructure. (Таб. 1).

Таблиця 1. Порівняння хмарних SBC

	Час налаштування дзвінка	Оцінка якості дзвінка (MOS Score)
Amazon Chime Voice Connector	Швидкий	Висока (Менше 4.34)
Twilio Elastic SIP Trunking	Швидкий	Хороша (Від 4.03- 4.34)
Azure Communication Services	Швидкий	Висока (Менше 4.34)
Dialogflow Telephony Gateway	Швидкий	Хороша(Від 4.03- 4.34)
Oracle Cloud Infrastructure	Швидкий	Висока (Менше 4.34)

Дана робота розглядається на основі таких елементів мережі: користувачі, корпоративна IP-мережа, хмарний SBC та Інтернет (Рисунок 1).

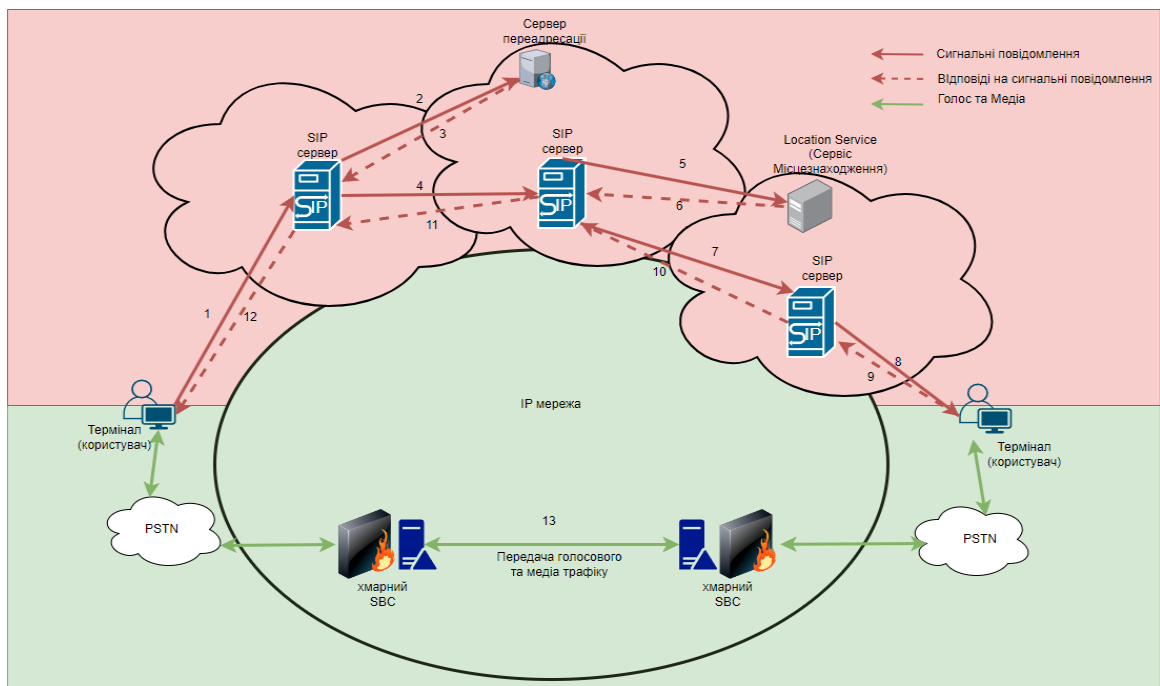


Рис. 1. Структурна схема елементів мережі.

Оцінка якості дзвінка (MOS) є широко використовуваною метрикою, яка може розраховуватися на основі різних факторів, таких як джиттер, затримка та інші параметри. Розрахунок використання ресурсів може бути виміряно як відсоток ресурсів, використаних під час обробки дзвінків [4,6]. Для оцінки якості дзвінка використана наступна формула (1):

$$MOS = 1 + (R - 1.5 * A) + (A * (A + 1) * B * C), \quad (1)$$

де R – рейтинг голосової якості (зазвичай від 1 до 5); A – джиттер (змiна затримки між пакетами); B – втрати пакетів (відсоток втрати); C – затримка (сума затримок в мілісекундах).

Валідація продуктивності та тестування. Для моделювання тестових SIP-сесій та генерації трафіку, реалізовано просту програму з використанням мови Java і бібліотеки JAIN-SIP. Код створює одну SIP-сесію та відправляє INVITE запит до сервера. У кодi створюється одна SIP-сесія та відправляється INVITE запит до сервера. Користувач може змінити адреси та

інші параметри для відповідності своїм потребам. Результат коду може виглядати наступним чином (рис. 2).

```
Sending an INVITE request to sip.example.com...

Response from the server:
HTTP/1.1 200 OK
Server: MySIPServer
Content-Length: 256
...

INVITE request successfully processed. The session is established.
```

Рис. 2. Результат програми.

Отримані експериментальні результати підтверджують високий рівень продуктивності хмарних SBC, і показують, що оптимізаційні стратегії [5], розглянуті у даному дослідженні, дозволяють покращити якість дзвінків і забезпечити ефективне використання ресурсів.

Висновки. Дане дослідження було спрямоване на проведення аналізу продуктивності хмарних SBC, виявлення можливих обмежень та пропозицію стратегій оптимізації з метою покращення загальної продуктивності, надійності та користувацького досвіду послуг SIP-транкінгу. Було продемонстровано, що використання SIP-транкінгу та хмарних SBC може значно покращити якість обслуговування в телекомунікаційних системах, що дає можливість оптимізувати маршрутизацію дзвінків та забезпечити безпеку комунікацій. Оцінка продуктивності хмарних SBC надала цінне уявлення про їхні можливості, а запропоновані стратегії оптимізації можуть стати конкретними рекомендаціями для поліпшення надання послуг SIP-транкінгу в хмарних середовищах.

Література

1. Романов О., Бурлака Г., Берестовенко О., Підпалый О. Технічні особливості побудови Li-Fi мережі за допомогою методів керування SDN/ Вісник ЧДТУ 2023; 0 (3): С:16-25; DOI: 10.24025/2306-4412.3.2023.284893
2. Kaul, S., & Jain, A. (2019). Study on the future of enterprise communication by cloud session border controllers (SBC). In: *International Conference on Intelligent Computing and Smart Communication* (pp. 407-414). Singapore: Springer.
3. Romaniuk, P.I. (2023). Cloud technologies: Analysis, perspectives, implementations. *Computer-Integrated Technologies: Education, Science, Production*, 50, 108-113.
4. Romanov, O., Nesterenko, M., Veres, L., Kamarali, R., Saychenko, I. Methods for calculating the performance indicators of ip multimedia subsystem (ims)/(2021) *Lecture Notes in Networks and Systems*, 152, pp. 229-256. DOI: 10.1007/978-3-030-58359-0_13
5. Tardaskina, T.M., & Hryshchuk, T.V. (2021). Features of use and development of cloud technologies in the digital economy. *Biznesinform*, 3, 254-260.
6. Romanov O., Nesterenko M., Mankivskyi V., Zhuk O. Principles of Building Modular Control Plane in Software-Defined Network// Part of the *Lecture Notes in Networks and Systems* book series (LNNS, volume 548), p. 333-335. https://link.springer.com/chapter/10.1007/978-3-031-16368-5_17

ALIGNMENT JITTER EVALUATION IN DIGITAL TRANSMISSION SYSTEMS USING QUEUING MODEL

Triska N.R.

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

ОЦІНЮВАННЯ ДЖИТЕРУ УЗГОДЖЕННЯ В ЦИФРОВИХ СИСТЕМАХ ПЕРЕДАЧІ З ВИКОРИСТАННЯМ МОДЕЛІ ЧЕРГ

В роботі розглядається можливість застосування математичного апарату теорії масового обслуговування (модель черг на обслуговування) з метою оцінювання параметрів узгодження швидкостей сигналів в цифрових системах передавання, зокрема, джитеру часу очікування.

The idea of applying queuing model known from the teletraffic theory to evaluate the signals alignment parameters (in particular, waiting time jitter) in the digital transmission systems has been considered.

Any interaction of digital signals (DS) is based on the data exchange (writing and reading) e.g. multiplexing/demultiplexing in PDH/SDH systems, switching centers (SC) connections, ATM cells and IP packets processing etc. It leads to the inevitable data losses (slips¹ of bits, bytes, frames, packets etc.) and requires some form of digital signals alignment [1, 2]. The alignment methods include bit/byte justification (stuffing), pointers (in SDH), controlled slips between SC, limitation of packet length. But only digital signals justification during multiplexing excludes slips as opposed to controlled frame slips between SC or packet loss.

There are well-known traditional approaches to evaluate the digital alignment effectiveness such as slip estimation in digital switching/transmission systems or PDV (packet delay variation) concept in packet networks [1, 2]. On the other hand, it may be useful to analyze the same processes from the other point of view – for example, by applying queuing model known from the classical teletraffic theory. In particular, we can consider alignment-related parameters such as

- PDV for packets and ATM cells,
- TIE accumulation in ISC² chain interconnection,
- the mean Time Error (TE) caused by a latency jitter in PDH/SDH systems as event flows in a queue for service.

To illustrate the approach, let us consider TE event flow under the assumption of Poisson (simplest) flow [3, 4]. Such a flow should meet the following general conditions:

- The flow is uniform, homogeneous; all events are equal.

^[1] Slip is the loss of data or the appearance of extra positions in a digital stream.

^[2] ISC – International Switching Center

Only the event arrivals (kick-off moments) are considered.

- No aftereffect (no or limited correlation between events on the different non-overlapping time intervals).
- Stationary time series/flow.

In general case, the stationarity condition is not met strictly for TE event flow because TE depends on time in the presence of constant frequency offset. But on the relatively short time intervals (corresponding to queue length) this dependence can be neglected and therefore TE flow can be considered locally stationary.

Let us consider as an example the conventional PDH multiplexing system $4 \times E12 = 1 E22$ ($4 \times 2048 \text{ kbit/s} = 8448 \text{ kbit/s}$)^[1]. The main parameters of writing/reading processes in the multiplexer elastic memory (EM) are:

- nominal E22 frame duration T_{frame} ;
- nominal E22 frame frequency f_{FRnom} ;
- nominal writing frequency of E12 tributary signal f_{Wnom} ;
- nominal reading frequency of E12 tributary f_{Rnom} .

One staffing bit is allocated for matching every E12 tributary signal in each E22 frame, i.e. maximal staffing frequency is equal to the nominal E22 frame frequency: $f_{\text{st max}} = f_{\text{FRnom}}$.

The nominal justification rate is defined as:

$$\rho_{\text{nom}} = (f_{\text{Rnom}} - f_{\text{Wnom}}) / f_{\text{st max}} = 0.4242$$

The real justification rate ρ can change over the interval $0 < \rho < 1$, so the bit staffing will occur irregularly. The real justification rate ρ can be considered as fractional frequency offset y of the writing/reading frequency difference $\Delta f_{\text{WR}} = (f_{\text{R}} - f_{\text{W}})$ relative the staffing rate $f_{\text{st max}}$.

The reciprocal of the justification rate $1/\rho$ shows how many frames are passed for one staffing on average, e.g. $1/\rho = 2.37$ signifies one staffing operation during two-three frames. The staffing irregularity causes additional waiting time jitter (or latency jitter) in the multiplexed signal [5].

It is interesting to evaluate the digital alignment processes and, in particular, waiting time jitter, using queuing theory. Any queuing system is defined by the following main parameters [4]:

- λ – arrival rate (request rate);
- μ – service rate;
- $\rho = \lambda/\mu$ – utilization factor of the server (e.g. elastic memory (EM), controller, etc.);
- t_s – service time;
- mean service time: $E(t_s) = 1/\mu$;

Stability condition of a queuing system is defined as $\lambda < \mu$ or $\lambda/\mu < 1$. Therefore, the system state can be described by the probability P:

$$\rho = \lambda/\mu \equiv \text{P [system is busy]}, \text{ and}$$
$$1 - \rho \equiv \text{P [system is idle]}.$$

^[1]The multiplexing principle and frame structure are defined in ITU-T Recommendation G.742.

In the case of waiting time jitter in the above-mentioned PDH multiplexing system $4 \times E12 = E22$, the queuing system parameters to be analyzed are: the mean waiting time of staffing;

- the mean time on the general justification time (mean waiting time + mean service time) and
- the waiting time deviation.

Request rate can be defined as

$$\lambda \equiv \Delta f_{WR} = (f_{Rnom} - f_{Wnom}),$$

where f_{Rnom} and f_{Wnom} – nominal writing and reading frequencies in the EM.

Service rate is $\mu \equiv f_{st\ max} = f_{FRnom}$.

Utilization factor of the PDH equipment EM:

$$\rho \equiv \lambda/\mu \equiv y \text{ (fractional frequency offset)}$$

We analyze TE event flow using $M/D/1$ queuing system model^[1] that means [4]:

- Poisson (simplest) arrival process;
- Deterministic service time;
- One server.

The calculations using this queuing model for the above-mentioned conditions gave the following waiting time jitter mathematical expectation (average value) $E(tw)$ and deviation $\sigma(tw)$:

$$E(tw) = 36.9 \mu s \approx 37 \% T_{frame}; \quad \sigma(tw) = 61.9 \mu s \approx 62 \% T_{frame}$$

To compare the obtained results with traditional “common sense” approach, the modelling of TIE during bit staffing process in PDH multiplexer was performed for the different values of the phase offset threshold (staffing request). The indirect estimation of the average waiting time jitter for $\rho_{nom} \equiv y$ is $36 \mu s$ that is close to queueing model $M/D/1$ results. The modelling has shown that the average latency (waiting time jitter) essentially depends on the used threshold level and is between $[26.7 \mu s, 42.6 \mu s]$.

The idea of using queuing models for digital transmission system parameters evaluation may be useful in both conventional and state-of-the art telecom equipment. The presented approach can be further developed and applied for the analysis and optimization of the various digital signals alignment processes.

References

1. N. Biriukov, N. Triska. Time and synchronization in telecoms. – Lecture Notes in Electrical Engineering. Volume 560: Advances in Information and Communication Technologies. Processing and Control in Information and Communication Systems. – Springer, 2019. ISSN 1876-1100. ISBN 978-3-030-16770-7. – p. 205-223.
2. N. Biriukov, A. Semenko, N. Triska. Alignment of the transport network digital streams. – Infocommunication and computer technology. Scientific journal, University “Ukraine”, № 2(02), 2021. – p. 64–80, DOI 10.36994/2788-5518-2021-02-02-05.
3. A.J. Hinchin. Works on the mathematical teletraffic theory, edited by B.V. Gnedenko. – Moscow, Phismathgiz, 1963. – 236 p.
4. L. Kleinrock. Queuing Systems, Volume I: Theory. – New York, Wiley, 1975.
5. D.L. Duttweiler. Waiting time jitter. – The Bell System Technical Journal, Vol. 51, No. 1, January, 1972. –p. 165-207.

^[1] The queue has an infinite storage capacity.

ULTRA-WIDEBAND MICROWAVE PRINTED MICROSTRIP DISC ANTENNA

Trubarov I.V.

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

НАДШИРОКОСМУГОВА МІКРОХВИЛЬОВА ДРУКОВАНА МІКРОСМУЖКОВА ДИСКОВА АНТЕНА

Здійснено проектування та оптимізацію несиметричної вібраторної антени із випромінювачем дискового типу, виконаної за друкованою технологією. Живлення антени здійснюється мікросмужковою лінією. Проведено моделювання роботи антени методом скінченних елементів. Шляхом оптимізації конструктивних параметрів антени досягнуто зменшення зворотних втрат у робочій смузі антени. Діапазон частот антени, в межах якого КСХ не перевищує 1.5, складає 2.1...4.7 ГГц. Збільшення робочої смуги антени досягається спеціальною формою випромінювача.

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 printed antenna types as well as design techniques used for their analysis and fabrication [1] – [3]. The basic radiating structure for this type of antennas is a patch microstrip antenna. However, these antennas are not omnidirectional and typically have gain of 6...9 dB [4 – 5]. To obtain omnidirectional directivity pattern, dipole [6] or monopole antenna [7] printed structures should be used.

In this paper, a microstrip monopole antenna is designed and simulated. The antenna is designed to operate in 2070...4700 MHz frequency band. As a radiating element, a disc topology was used. Such antennas can be considered as a variation of a monopole microstrip antenna, whose radiating element has not a linear, but a specific shape. This approach provides the ability of the antenna to operate in wide frequency band. The antenna, designed in the present work, can be used in mobile ISM band communication systems, such as Wi-Fi, Bluetooth or Zigbee applications. For the simulation and optimization of the antenna, finite-element method (FEM) was used.

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

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 manifests pertinent performance in the 1.1...4.7 GHz frequency range.

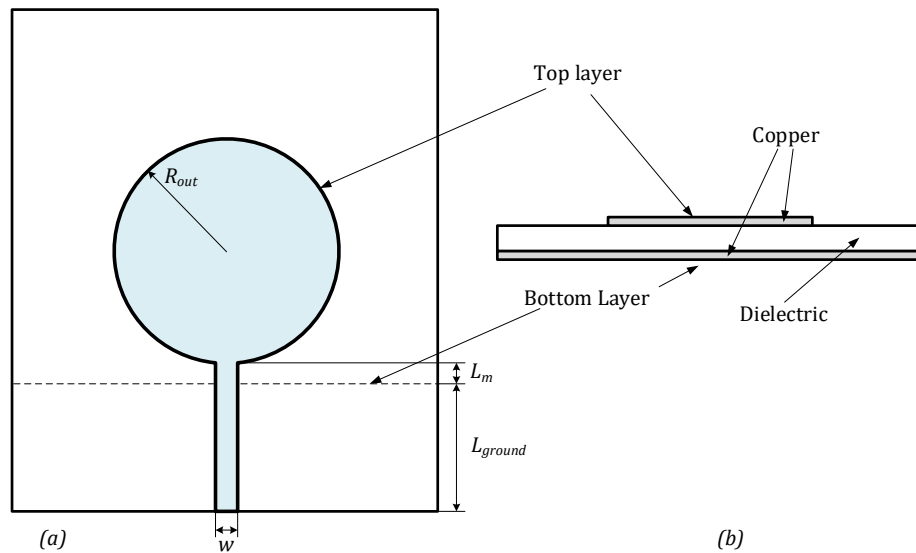


Fig.1. Dimensions of a microstrip monopole antenna. (a) Antenna dimensions. (b) Side view of the antenna

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: L_m , R_{out} .

As a result of the optimization process, the following values were obtained for the antenna geometry $L_{ground} = 30$ mm; $L_m = 0.2$ mm; $w = 2.9$ mm; $R_{out} = 30$ mm. The model of the antenna is shown in Fig. 2 (a), and Fig. 2 (b) shows the VSWR of the antenna. It can be seen that VSWR is lower than 1.5 in the 2.1...4.7 GHz continuous frequency band.

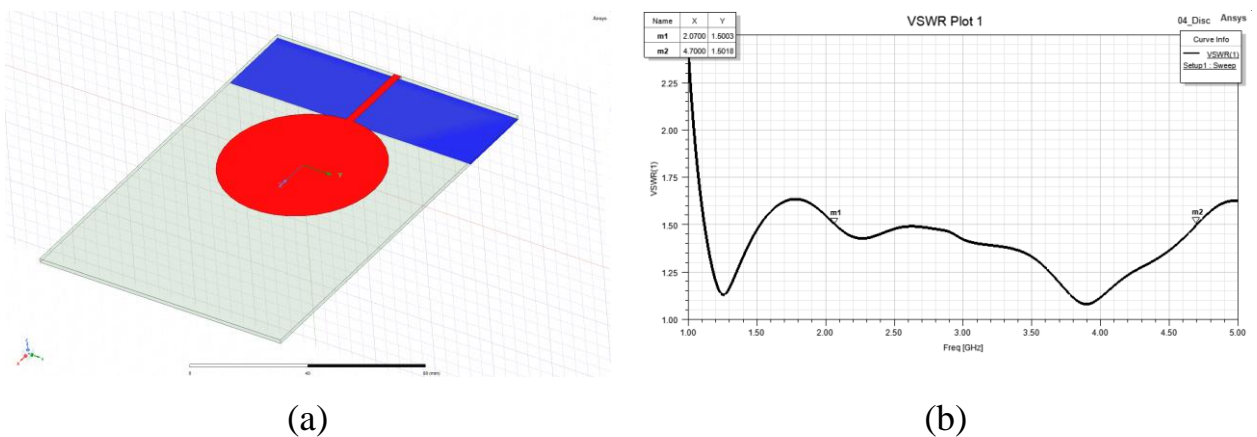


Fig.2. (a) Model of the antenna. (b) Return loss of the antenna.

The antenna with a disc 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 maximum gain is 4.6 dBi and observed within the cone of the highest directivity at $\theta = 46^\circ$. The distortion of the radiation pattern is caused by the dielectric layer of PCB and the disc shape of the radiating element.

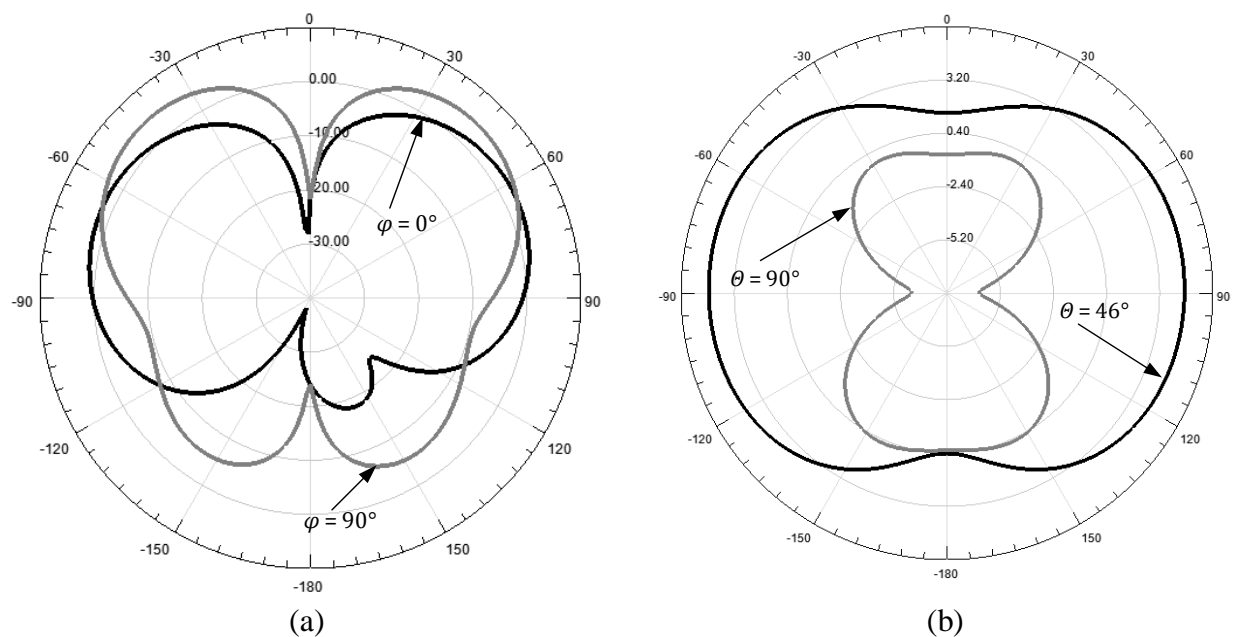


Fig.3. Directivity pattern of the antenna. (a) E-plane. (b) H-plane.

The antenna designed in the present research is small-sized and easily fabricated. VSWR value is less than 1.5 within the operating bandwidth 2.1...4.7 GHz. The antenna gain in the maximum of the main lobe is 4.6 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 areas.

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 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
5. 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.
6. Trubarov I.V. Printed Dipole Antenna for 2.4 GHz Frequency Band // XVII International Scientific Conference "Modern Challenges in Telecommunications" MCT-2023. Conference proceedings. Kyiv. Igor Sikorsky Kyiv Polytechnic Institute, 2023 – pp. 96 – 98. – ISSN(print)2663-502X.
7. Trubarov I.V. Microstrip Ring Antenna for 2.4 GHz Frequency Band // XVII International Scientific Conference "Modern Challenges in Telecommunications" MCT-2023. Conference proceedings. Kyiv. Igor Sikorsky Kyiv Polytechnic Institute, 2023 – pp. 99 – 101. – ISSN(print)2663-502X.

MUTUAL COUPLING COEFFICIENTS BASIC AND HIGHER MODES OF SPHERICAL DIELECTRIC RESONATORS

Trubin A. A.

*National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"
E-mail: atrubin9@gmail.com*

КОЕФІЦІЄНТИ ВЗАЄМНОГО ЗВ'ЯЗКУ ОСНОВНИХ ТА ВИЩИХ КОЛИВАНЬ СФЕРИЧНИХ ДІЕЛЕКТРИЧНИХ РЕЗОНАТОРІВ

Вперше досліджуються коефіцієнти взаємного зв'язку між коливаннями основних та вищих типів. Знайдено нові загальні аналітичні вирази для коефіцієнтів взаємного зв'язку діелектричних резонаторів сферичної форми. Досліджуються властивості зв'язаних коливань нижчих типів з коливаннями шепочущей галереї. Результати досліджень є основою для побудови різноманітних оптичних пристроїв для систем оптичного зв'язку.

Today, high-quality spherical dielectric resonators are important elements suitable for further use in a variety of communication devices [1 – 8]. Currently, DRs with whispering gallery oscillations are mainly used in the optical and infrared ranges [3 – 5]. These oscillations have a very high quality factor, but their frequency spectrum is quite dense. One of the effective ways to rarefy the frequency spectrum is to use coupled resonators with different types of natural oscillations. In addition, in some devices, such as power dividers, it is assumed that DRs with different types of oscillations will be used. To model the electromagnetic parameters of such devices, it is necessary to know the coefficients of mutual coupling between resonators of different types. In this case, it is desirable to have analytical expressions for coupling coefficients, since the speed of calculating the parameters of more complex structures based on them increases many times.

In works [9, 10], the coefficients of mutual coupling of spherical DR in open space already have been studied. We found general analytical expressions for the coupling coefficients of DRs of different types, obtained in the form of complex integral expansions. It was shown that the above general formulas can be calculated in quadratures, in the form of a series, using a generalization of the Sommerfeld integral [11], however they require the calculation of rather cumbersome coefficients expressed through 3-j Wigner symbols. This study examines simpler special cases of accurately calculating coupling coefficients between spherical DRs of different sizes, one of which is excited by the main magnetic or electrical mode of oscillations. The natural oscillations of the second DR can be anything. As a result, we obtained new exact analytical formulas for complex coupling coefficients: $\kappa_{12} = \kappa_{12}(\Delta\theta, \Delta\alpha, k_0\Delta r)$ without additional expansions. Where in the spherical coordinate system of the first DR, the vector $(\Delta r, \Delta\theta, \Delta\alpha)$ determines the coordinates of the center of the second resonator.

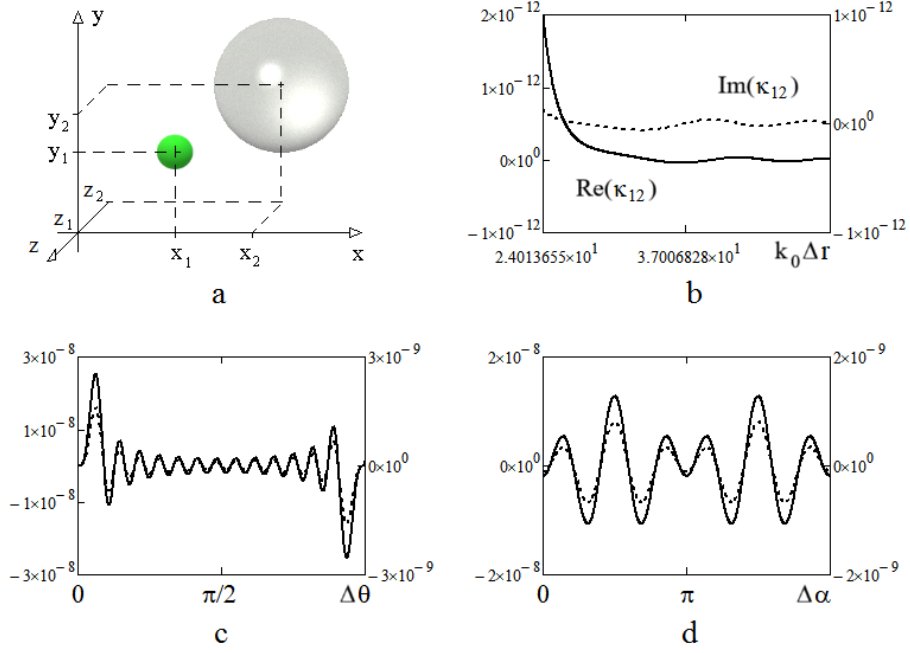


Fig. 1. Different spherical DR with main and higher oscillations (a). The coupling coefficients of two different DR with $H_{1,m,1}$ and $H_{5,30,1}$ as functions of the distance between resonator centers (b) ($\Delta\theta = 1,3$; $\Delta\alpha = 2$); as a function of changing angles (c, d) ($\Delta\alpha = 0$ (c); $\Delta\theta = 1,4$ (d); $k_0\Delta r = 17$) for $\varepsilon_{1r} = 25$; $\varepsilon_{2r} = 2,25$.

On Fig. 1 shows an example of calculating the dependences of the DR coupling coefficients, the dimensions of one of which correspond to the possibility of the existence of the main magnetic oscillation H_{1m1} , and the second the existence of a magnetic oscillation of the whispering gallery $H_{5,30,1}$. The dependence of the real (left ordinate axis) and imaginary part (right ordinate axis) on the distance between the centers of the resonators is shown in Fig. 1, b, and with variations in angular variables, in Fig. 1, c, d. Solid lines show the dependences of the real part, and dotted lines show the dependences of the imaginary part of the coupling coefficients. As one would expect, the maximum values of the real part of the coupling coefficients, corresponding to the splitting of the frequencies of coupled oscillations, in most cases are established in the region adjacent to the surface of the resonator with whispering gallery oscillations (Fig. 1, b). As the resonators move away from each other, the coupling coefficients quickly decrease.

The general picture of the distribution of the real part of the mutual coupling coefficients of resonators in the plane $|k_0\Delta z| = 0,1$ for different types of oscillations is shown in Fig. 2, a–c.

Thus, the obtained analytical expressions for the mutual coupling coefficients of the basic and higher types of spherical DR oscillations make it possible to construct electromagnetic models of a wide class of devices in the optical and infrared range.

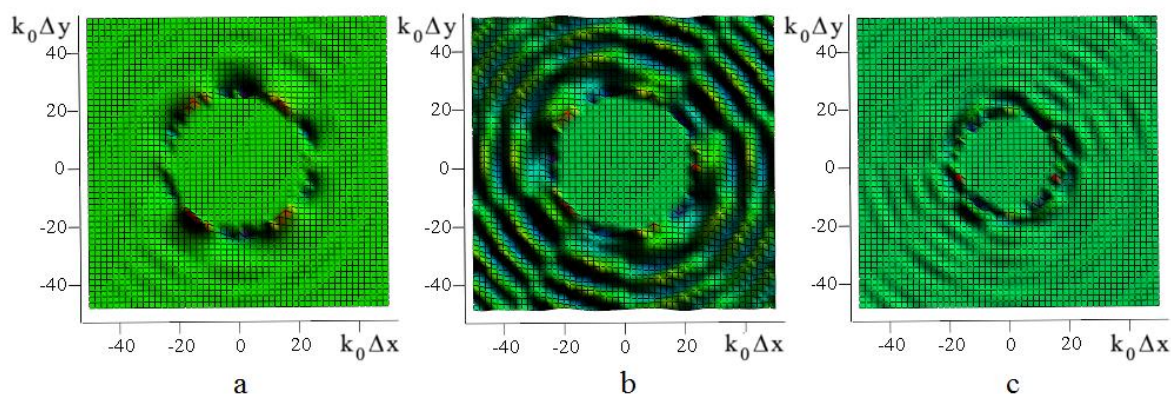


Fig. 2. Distribution of the real part of the coupling coefficients from the coordinates of the resonators in the plane (x, y) for $H_{1,1,1}$ and $H_{5,30,1}$ oscillations (a); $H_{1,0,1}$ and $H_{5,30,1}$ oscillations (b); $H_{1,0,1}$ and $E_{5,30,1}$ oscillations (c).

The considered systems of coupled resonators can be used in various elements of optical communication systems: antennas, sensors, channel switches, etc.

References

1. P. Salzenstein, M. Mortier, H. Serier-Brault, H. Remi, A. Coillet, Y.K. Chembo, A. Rasoloniaina, Y. Dumeige, P. Feron, Coupling of high quality factor optical resonators // *Physica Scripta*, vol. 157, 2013, pp. 014-024.
2. Mitsui T., Onodera T., Wakayama Y., Hayashi T., Ikeda N., Sugimoto Y., Takamasu T., Oikawa H. Influence of micro-joints formed between spheres in coupled-resonator optical waveguide // *Optics Express*. 2011 , Vol. 19, No. 22. PP. 22258-22267.
3. Xifré-Pérez E., Domenech J.D., Fenollosa R., Munoz P., Capmany J., Meseguer F. All silicon waveguide spherical microcavity coupler device // 2011/ Vol. 19, No. 4 / *Optics Express*. PP. 3185-3192.
4. Righini G. C., Dumeige Y., Feron P., Ferrari M., Nunzi Conti G., Ristic D., Soria S. Whispering gallery mode microresonators: Fundamentals and applications // *Rivista del Nuovo Cimento*, 2011, vol. 34, N. 7, pp. 435 - 488.
5. Astratov V. N. Ch. Fundamentals and Applications of Microsphere Resonator Circuits. *Photonic Microresonator Research and Applications*. Springer. 2010. PP. 423-457.
6. Thompson D.B., Keating D.A., Guler E., Ichimura K., Williams M.E., Fuller K.A. Separation-sensitive measurements of morphology dependent resonances in coupled fluorescent microspheres // *Optics Express*. 2010 , Vol. 18. No. 18. PP. 19209 - 19218.
7. A. Kirichenko, Yu. Prokopenko, Yu Filipov, N. Cherpak "Qasioptical solid-state resonators" Kiev: Naukova dumka, 2008, 286 p.
8. Chen Z., Taflove A., Backman V. Highly efficient optical coupling and transport phenomena in chains of dielectric microspheres // February 1, 2006 / Vol. 31, No. 3 / *Optics Letters*. PP. 389-391.
9. Trubin A.A. Coupling coefficients of the Spherical Dielectric Micro-resonators with Whispering gallery modes // *Bulletin of NTUU "KPI" ser. Radiotechnique, Radioaparatus Building*. 2015. N.62, pp. 49-61.
10. Trubin A.A. Coupling coefficients of different Spherical Dielectric Microresonators // *Information and Telecommunication Sciences*, 2018, V. 9, No 1, pp. 49-56.
11. A.A. Trubin. *Lattices of Dielectric Resonators*. Springer International Publishing Switzerland – 2016 – 171 p.

PERTURBATION THEORY OF COUPLED OSCILLATION OF RESONATORS WITH ACTIVE AND ABSORBING DIELECTRIC

Trubin A. A.

National Technical University of Ukraine

“Igor Sikorsky Kyiv Polytechnic Institute”

E-mail: atrubin9@gmail.com

ТЕОРІЯ ЗБУРЕНЬ ЗВ'ЯЗАНИХ КОЛИВАНЬ РЕЗОНАТОРІВ З АКТИВНИМ ТА ПОГЛИНАЮЧИМ ДІЕЛЕКТРИКОМ

Розвивається теорія збурень, придатна для опису зв'язаних коливань діелектричних резонаторів, виконаних з активних діелектриків та діелектриків із втратами. Знайдена система рівнянь яка визначає амплітуди та частоти резонаторів та в окремих випадках збігається зі знайденою раніше.

Досліджуються зв'язані коливання діелектричних резонаторів різних видів. Отримані закономірності добре согласуються з результатами, знайденими в інших публікаціях на основі застосування чисельних методів та експериментальних досліджень. Представлені результати є основою для розрахунку та побудови широкого класу різноманітних оптичних модуляторів, перемикачів потужності, та сенсорів для систем оптичного зв'язку і інтернету речей.

It is known that the physical conditions in the DR can be implemented in such a way that energy from an external source is transferred to the field excited in its material. It is convenient to describe such resonators by introducing into consideration the concept of active dielectrics, materials in which the imaginary part of the dielectric constant can take positive values. In works [1 - 4], coupled systems of similar waveguides and resonators have already been considered, carried out using numerical methods, simulation and experimentally.

Previously [5], we considered dielectric resonators made of an ideal lossless dielectric whose dielectric constant is a purely real quantity. In this report, using perturbation theory for Maxwell's equations, coupled oscillations of resonators, the material of which is a complex function $\tilde{\epsilon}_n = \epsilon'_n + i\epsilon''_n$, are studied, the imaginary part of which can take both positive and negative values. The resulting system of equations is used to study coupled oscillations of DRs made of an active dielectric and a dielectric with power losses. The found system of equations coincides with that obtained earlier [5] for $\epsilon''_n = 0$.

The simplest systems are considered, consisting of two coupled resonators, the material of one of the resonators is absorbing $\epsilon''_n < 0$, and the second is active $\epsilon''_n > 0$. Resonators with fundamental magnetic oscillations, as well as resonators with whispering gallery oscillations are investigated. (Fig. 1, 2).

On Fig. 1 shows the solutions of the equation systems for coupled oscillations of the absorbing and active DR with variation of the imaginary part of the dielectric constant of the second resonator.

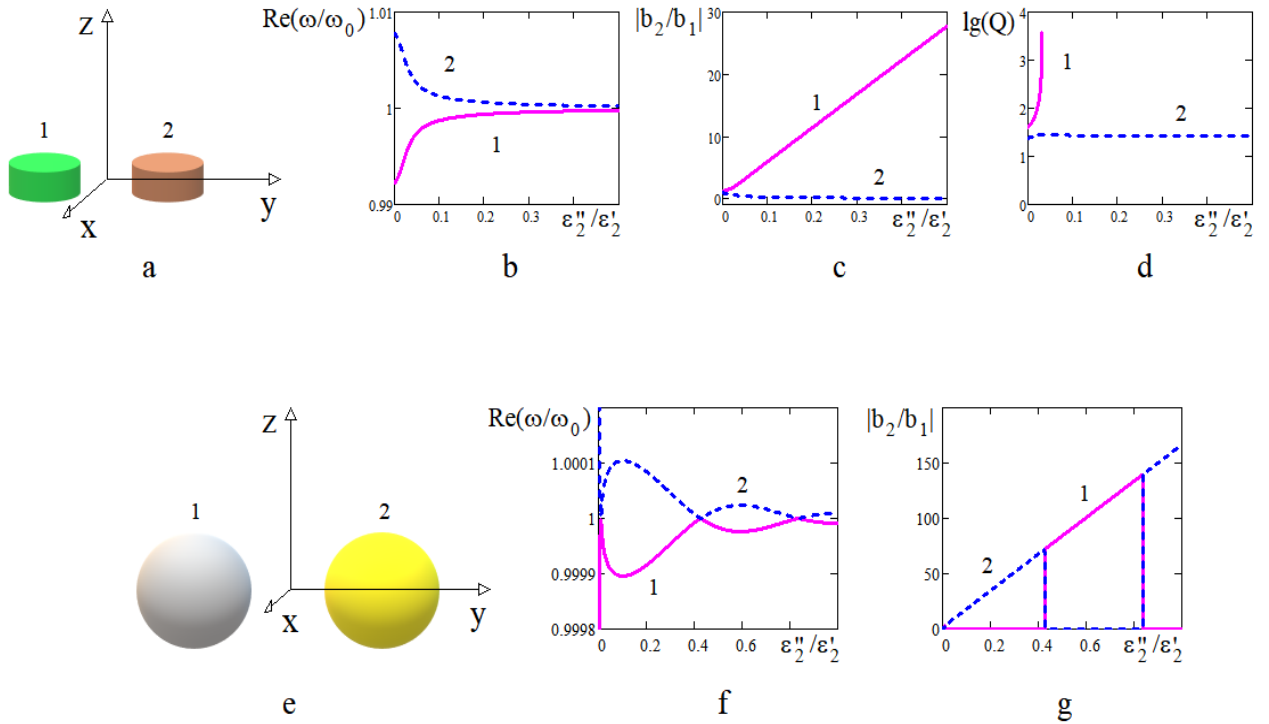


Fig. 1. Different cylindrical DR with main oscillations H_{101} (a) ($\epsilon_1''/\epsilon_1' = -0,01$; $\epsilon_{1r} = \epsilon_{2r} = 36$; $\Delta_1 = \Delta_2 = 0,4$; $f_0 = 10\text{GHz}$; $\Delta x = \Delta z = 0$; $\Delta y = 10\text{mm}$). Different spherical DR with a whispering gallery mode $H_{26,26,1}$ (e) ($\epsilon_{1r} = \epsilon_{2r} = 2,4$; $\Delta x = \Delta z = 0$; $k_0 \Delta y = 40$). The coupling frequencies (b, f); amplitude ratio (c, g) quality factor of coupled oscillations (d) as functions of the complex dielectric constant tangent function of the second DR (a) ($\epsilon_1''/\epsilon_1' = -0,01$).

As follows from the data obtained, an increase in the imaginary part of the dielectric constant for resonator 2 leads to a decrease in the detuning between frequencies (Fig. 1, b, f). The amplitudes of coupled oscillations are distributed in such a way that only one of the resonators of the system is excited (c, g). In this case, the quality factor of one of the coupled oscillations increases exponentially, and the quality factor of the other coupled oscillation remains approximately constant (d).

When using resonators with whispering gallery mods, the noted qualitative patterns of changes in the parameters of coupled oscillations are preserved (Fig. 1, e - g), however, the dependences of the frequencies become more complex functions of the dielectric parameters (Fig. 1, f).

On Fig. 2 shows the results of calculating the frequencies, amplitudes and quality factors of coupled oscillations of 3 cylindrical DRs with a whispering gallery oscillations $EH_{1,20,1}$.

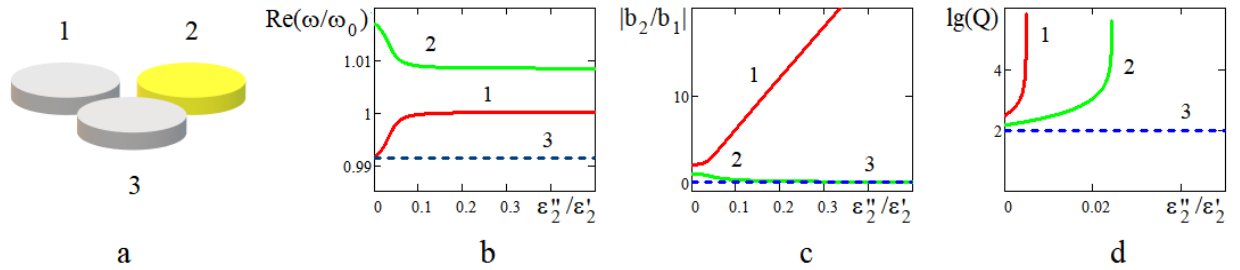


Fig. 2. 3 different cylindrical DR with a whispering gallery mode $EH_{1,20,1}$ (a) ($\epsilon'_{1r} = \epsilon'_{2r} = \epsilon'_{3r} = 9$; $k_0\Delta r = 22$ $\Delta_1 = \Delta_2 = \Delta_3 = 0,2$). The coupling frequencies (b); amplitude ratio (c) quality factor of coupled oscillations as functions of the complex dielectric constant tangent function of the second DR (a) ($\epsilon''_1 / \epsilon'_1 = \epsilon''_3 / \epsilon'_3 = -0,01$).

The obtained patterns of amplitude distribution confirm the previously discovered effect [6, 7], the essence of which is that coupled oscillations in complex lattices consisting of various types of DR are broken down into oscillations of individual sublattices. All resonators in each individual sublattice are characterized by the same shape and the same parameter values.

Thus, using perturbation theory, we have obtained a new system of equations that describes the general patterns of behavior of multi-element lattices with DR performed by their various dielectrics. Considered DR lattices can find practical application in multiplexers, amplifiers, channel switches and other devices of infrared and optical communication systems.

References

1. Hlushchenko A.V., Novitsky D.V., Tuz V.R. Trapped mode excitation in all-dielectric metamaterials with loss and gain // Physical Review B **106**, 155429 (2022) 2022. PP. 155429-1 – 155429-9.
2. S. Phang, A. Vukovic, G. Gradoni, P. D. Sewell, T. M. Benson, S. C. Creagh. Theory and Numerical Modelling of Parity-Time Symmetric Structures in Photonics: Boundary Integral Equation for Coupled Microresonator Structures. Chapter. Recent Trends in Computational Photonics . November 2017. pp 207–233. https://link.springer.com/chapter/10.1007/978-3-319-55438-9_7.
3. Bo Peng, S. K. Özdemir, F. Lei, F. Monifi, M. Gianfreda, G. L. Long, S. Fan, F. Nori, C. M. Bender, L. Yang. Parity–time–symmetric whispering-gallery Microcavities // Nature Physics. Vol. 10. May 2014. www.nature.com/naturephysics , pp. 394 - 398.
4. C. E. Rüter, K. G. Makris, R. El-Ganainy, D. N. Christodoulides, M. Segev, D. Kip. Observation of parity–time symmetry in optics // Nature Physics. Vol. 6, March 2010, pp. 192 – 195. www.nature.com/naturephysics.
5. A.A. Trubin. Study of electromagnetic oscillations in a system of coupled dielectric resonators using perturbation theory // Bulletin of NTUU "KPI" ser. Radiotechnique. 1987. Vol. 24, pp. 42 - 45 (in russian).
6. A.A. Trubin. Eigenoscillations lattices of different dielectric microresonators // "Modern Challenges in Telecommunications", Kiev. 2019. pp. 99-102.
7. A.A. Trubin. Modeling of optical topological insulators on lattices of coupled dielectric resonators // "Modern Challenges in Telecommunications", Kiev. 2022. pp. 66-68.

УДК 621.396.1

**СПОСІБ СУМІСНОЇ ПРОСТОРОВО-ЧАСОВОЇ ТА МОДЕМНОЇ
КОМПЕНСАЦІЇ СТРУКТУРНОЇ ЗАВАДИ ЦИФРОВОЇ РАДІОЛІНІЇ
З ШИРОКОСМУГОВИМ ФАЗОМАНІПУЛЬОВАНИМ СИГНАЛОМ**

Василенко С.В., Єрохін В.Ф.

Інститут спеціального зв'язку та захисту інформації

Національного технічного університету України

“Київський політехнічний інститут імені Ігоря Сікорського”, Україна

E-mail: vasylenko.iszzi@gmail.com

**METHOD OF COMBINED SPACE-TIME AND MODEM
COMPENSATION OF STRUCTURAL INTERFERENCE OF A DIGITAL RADIO
LINE WITH BROADBAND PHASE-MANIPULATED SIGNALS**

In order to compensate for the structural interference in the input mixture of the broadband phase-manipulated signal and the structural interference, the paper proposes the combined use of space-time and modem compensation.

З метою підвищення якості прийому сигналів в умовах дії активних завад широкосмугові системи радіозв'язку з двійковою фазовою маніпуляцією використовують адаптивні антенні решітки (ААР). При цьому виникає необхідність у мінімізації середньоквадратичної помилки прийнятого сигналу, що може бути досягнуто за рахунок динамічного управління параметрами ААР.

Для вирішення цього завдання у роботах [1–5] пропонується для управління ААР використовувати широкосмугові сигнали на основі квазіортогональних послідовностей з хорошими автокореляційними властивостями. При цьому згортка сигналу виконується у демодуляторі приймача широкосмугового сигналу та не передбачає жодних процедур компенсації завад.

В роботі [6] пропонується у демодуляторі додатково здійснювати сумісну просторово-часову та модемну компенсацію структурної завади. При цьому одночасна відбувається згортка корисного сигналу у вхідній суміші широкосмугового фазоманіпульованого сигналу та компенсація структурної завади з подальшою демодуляцією та формуванням оцінки завади.

Рішення поставленої задачі досягається тим, що з вхідної суміші широкосмугового сигналу та структурної завади, яка надходить на вхід ААР, шляхом згортки, оцінки початкової фази та амплітуди, здійснюється формування оцінки структурної завади, яка в подальшому використовується

для формування так званої “нев’язки” за допомогою якої і відбувається управління діаграмою спрямованості ААР.

Запропонований спосіб може бути реалізований за допомогою пристрою, структурна схема якого представлено на рис. 1.

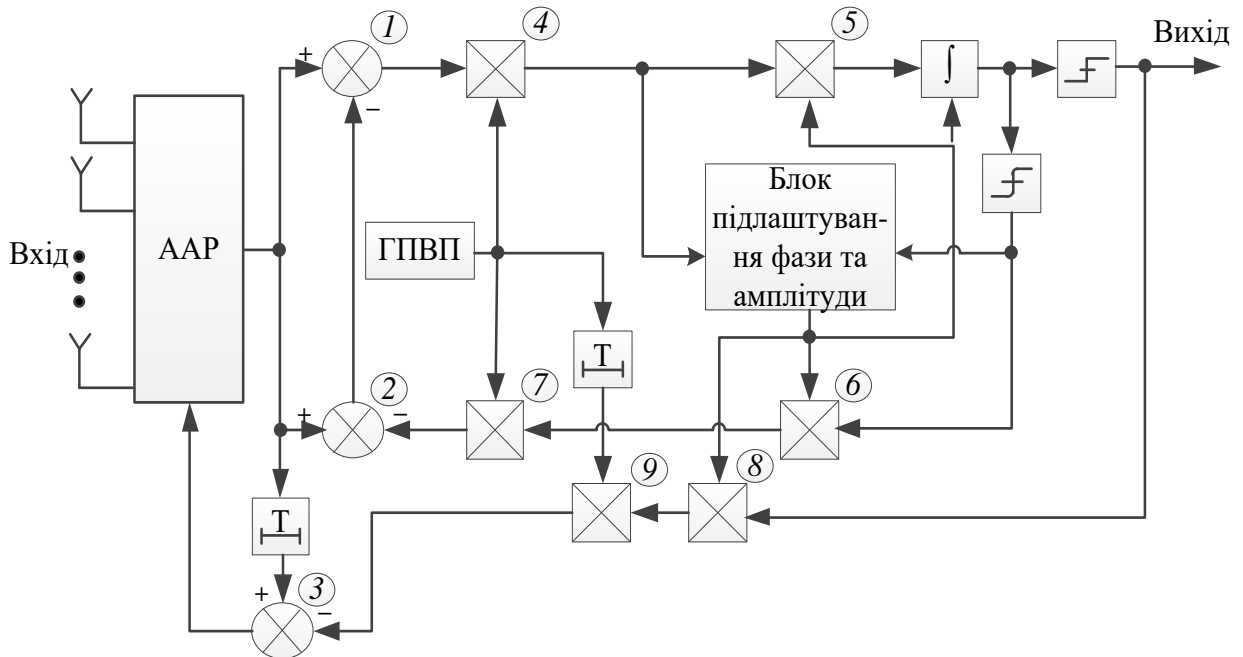


Рис. 1. Спосіб сумісної просторово-часової та модерної компенсації структурної завади цифрової радіолінії з широкосмуговим фазоманіпульованим сигналом.

Нехай на виході блоку ААР присутнє спостереження, що містить корисний широкосмуговий сигнал з двійковою фазовою маніпуляцією, структурну заваду та адитивний білий гаусівський шум:

$$\pi(k)(-1)^k \lambda_c(t) + \lambda_s(t) + n(t),$$

- де: $\pi(k)$ – псевдовипадкова послідовність на k -му інформаційному тактовому інтервалі, що приймає значення ± 1 ;
 $r = \overline{0,1}$ – інформаційний дискретний параметр сигналу;
 λ_c, λ_s – дифузійні марківські процеси, що описують сигнал та заваду;
 $n(t)$ – адитивний білий гаусівський шум.

Спостереження з виходу блоку ААР надходить на блок віднімання 1, де від нього віднімається оцінка неперервних неінформаційних параметрів сигналу $\lambda_c^*(t)$, яка надходить з блоку 2. Отримане спостереження у блоці 4 перемножується на псевдовипадкову послідовність (ПВП), яка далі у блоці 5 перемножується на опорне коливання з оцінкою амплітуди і початкової фази сигналу $\lambda_c^*(t)$. Після обнулення послідовності у кінці кожного тактового інтервалу інтегратором на виході обмежувача буде присутня величина

$th(\xi) = \hat{r}^*$, яка спочатку перемножується з $\lambda_c^*(t)$ у блоці 6, а потім – з ПВП у блоці 7 та матиме вигляд:

$$\pi(k) \left[th(\xi) \lambda_c^*(t) \right].$$

Для отримання сигналів керування ААР оцінка завади у блоках 8 та 9 перемножується з $\lambda_c^*(t)$ та ПВП відповідно та у блоці 3 віднімається затримана вхідна суміш. При цьому на виході блоку 3 отримуємо:

$$\pi(k-1) \left[(-1)^{r_{k-1}} \lambda_c(t-T) - (-1)^{r_{k-1}^*} \lambda_c^*(t-T) \right] + \lambda_s(t-T) + n(t).$$

Зважаючи на те, що сигнал представляє собою коливання з двостановою фазовою маніпуляцією, рішення про значення дискретного параметра r_{k-1}^* корисного сигналу у блоці прийняття рішень ААР буде прийматися за правилом:

$$r_{k-1}^* = \begin{cases} 0, & \gamma = \int_{t_{k-1}}^{t_k} \left[\left((-1)^{r_k} \lambda_c(t) - (-1)^{r_k} \lambda_c(t) + th(\xi) \lambda_c^*(t) \right) \lambda_c^*(t) + \hat{n}(t) \right] dt < 0; \\ 1, & \gamma \geq 0. \end{cases}$$

Отже, використання способу сумісної просторово-часової та модемної компенсації структурної завади, за рахунок реалізації процедури згортки корисного сигналу та компенсації структурної завади, а також формування вектора “нев’язки” для управління діаграмою спрямованості ААР, дозволить покращити процедуру компенсації структурної завади у вхідній суміші широкопasmового фазоманіпульованого сигналу та структурної завади цифрової радіолінії з широкопasmовим фазоманіпульованим сигналом.

Література

1. Риглер Р., Комптон Р. Адаптивная антенная решетка для подавления помех / Р. Риглер, Р. Комптон. – М. : ТИИЭР, 1973, том 61, № 6, с. 75 – 86.
2. Комптон Р. Адаптивная антенная решетка в широкополосной системе связи / Р. Комптон. – М. : ТИИЭР, 1978, том 66, № 3, с. 23 – 34.
3. Родимов А., Поповский В. Статистическая теория поляризационно-временной обработки сигналов и помех в линиях связи / А. Родимов. – М. : Радио и связь. 1984. 272 с.
4. Монзинго Р., Миллер Т. Адаптивные антенные решетки: Введение в теорию: Пер. с англ. / Р. Монзинго, Т. Миллер. – М. : Радио и связь, 1986. – 448 с.
5. Уидроу П., Стирнз С. Адаптивная обработка сигналов / П. Уидроу, С. Стирнз. – М. : Радио и связь. 1989. 440 с.
6. Пат. 155262 Україна, Н04В 1/10. Спосіб сумісної просторово-часової та модемної компенсації структурної завади цифрової радіолінії з широкопasmовим фазоманіпульованим сигналом / Борсук О.О., Василенко С.В., Єрохін В.Ф., заявник, власник Борсук О.О., Василенко С.В., Єрохін В.Ф. – № у 2023 01183; заявл. 22.03.2023; опубл. 07.02.2024, Бюл. № 6.

МОДЕЛЮВАННЯ ДІЕЛЕКТРИЧНОЇ РЕЗОНАТОРНОЇ АНТЕНИ ДІАПАЗОНУ 4 ГГц

Авдєєнко Г. Л., Наритник Т. М., Шевцов К. О.
 Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
 E-mail: django2006@ukr.net

SIMULATION OF THE 4 GHz BAND DIELECTRIC RESONATOR ANTENNA

The results of modeling a dielectric resonator antenna which consists of a section of a microarray line and a disk dielectric resonator using the CST Studio Suite software in the 4 GHz range are presented. This thesis will be useful for manufacturers of antennas and antenna devices in the microwave range.

Діелектрична резонаторна антена (ДРА) складається з мікросмужкової лінії та діелектричного резонатора, який виготовляється з матеріалу з низькими втратами та високою відносною діелектричною проникністю (ϵ_{DRA}) різної геометричної форми – циліндричної, прямокутної, сферичної, напівсферичної напіврозрізної циліндричної тощо (рис.1). Резонансні частоти такої ДРА залежать від розміру, форми та діелектричної проникності матеріалу ДР. За останні 40-50 років діелектричні резонатори знайшли широке застосування при створенні широкого класу пристроїв мікрохвильового діапазону, таких як: смугопропускні та режекторні фільтри, дуплексири, гетеродини тощо [1].

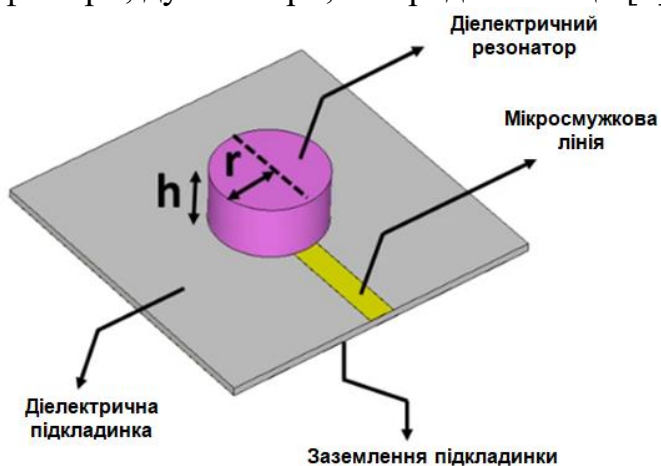


Рис.1. Конструкція діелектричної резонаторної антени: h – висота резонатора, r – радіус резонатора.

ДРА характеризуються малими габаритними розмірами, просторою конструкції, високою ефективністю випромінювання електромагнітних хвиль (ЕМХ) і низькою вартістю виробництва, що робить їх дуже перспективними для застосування в системах бездротового зв'язку. ДРА можуть бути розроблені для прийому/передавання ЕМХ як з лінійною, так й з коловою поляризацією [2].

Типові параметри ДРА мають наступні значення [3]:

- Висока діелектрична проникність матеріалу ДР: $\epsilon_{DRA} = (20...100) \pm (1..5)\%$;
- Висока ефективність випромінювання ДР ($\approx 95\%$) за рахунок відсутності втрат у провідниках або поверхневій хвилі ;
- Висока добротність Q ДР: до 10000 ($f = 10$ ГГц);

- Широкий діапазон температурного коефіцієнта резонансу частота: $\tau_f = (-12...+30)$ ppm/°C та його допуск $\tau_f = \pm 0,5; \pm 1,0; \pm 2,0$ ppm/°C.

Методика моделювання ДРА за допомогою програмного пакету CST Studio Suite передбачає виконання наступних кроків:

1. Вибір форми ДР, його розмірів та розрахунок його резонансної частоти.

2. Вибір матеріалу підкладки та її габаритних розмірів.

3. Розрахунок параметрів мікросмушкової лінії (довжина, ширина, товщина).

4. Створення топології ДРА, підключення вимірювального порту.

5. Налаштування параметра симулятора та здійснення моделювання та розрахунків параметрів ДРА: частотної характеристики коефіцієнту відбиття S_{11} , діаграм спрямованості (ДС) в далекій хвильовій зоні, ширини.

Резонансна частота ДРА може бути приблизно (з точністю 5-10%) може бути оцінена за наступною формулою (в режимі збудження електромагнітної хвилі TEM_{11δ}):

$$f_r = \frac{c}{2\pi r \sqrt{\varepsilon_{DRA}}} \left[1.71 + \frac{r}{h} + 0.1578 \left(\frac{r}{h} \right)^2 \right], \quad (1)$$

де f_r визначається в ГГц, r та h в мм, ε_{DRA} – діелектрична проникність матеріала діелектричного резонатора, c – швидкість поширення ЕМХ у вільному просторі.

Прийmemo параметри r та h рівними : $r = 10$ мм, $h = 10$ мм. Тоді, при використанні діелектрика типу Alumina Ceramic, що має $\varepsilon_{DRA} = 9,9$, $\text{tg}\delta_{DRA} = 0,0001$, згідно (1) отримаемо розрахункову частоту:

$$f_r = \frac{3 \cdot 10^8}{2 \cdot 3,14 \cdot 10 \cdot \sqrt{9,9}} [1.71 + 1 + 0.1578] \approx 4.349 \text{ ГГц}. \quad (2)$$

У якості матеріалу підкладки обрано Rogers RT Duroid 5800, який має відносну діелектричну проникність $\varepsilon = 2,2$, $\text{tg}\delta = 0,001$, товщину діелектрика $H = 1,52$ мм та товщину металізації однієї (нижньої) сторони $t = 0,035$ мм. Ширина та довжина підкладки обрані рівними відповідно $S_L = S_W = 60$ мм та товщину металізації.

Користуючись онлайн калькулятором параметрів мікросмушкової лінії з урахуванням параметрів підкладки, для розрахункової частоти 4,3 ГГц та хвильового опору лінії $Z = 50$ Ом отримано ширину цієї лінії, що збуджує ДР, яка дорівнює $W = 4,65$ мм. Довжину цієї лінії обрано рівною $L = 40$ мм, що забезпечує перекриття нижньої поверхні ДР.

Після створення відповідно до рис.1 топології ДРА, налаштування вимірювального порту та симулятора, було отримано для діапазону робочих частот 3,8...4,6 ГГц частотну характеристику модуля коефіцієнту відбиття, що зображена на рис.2, а на рис.3 – ДС ДРА. Мінімум коефіцієнта $S_{11} = -42$ дБ припадає на частоту 4,156 ГГц, що на 3,7% менше за розрахункове значення, отримане за формулою (2). Ширини смуги пропускання ДРА за рівнем – 3 дБ складає приблизно $\Delta f = 12,1$ МГц.

Аналіз ДС ДРА на рис.3 показує, що антена має спрямоване випромінювання у напрямку, перпендикулярному площині антени.

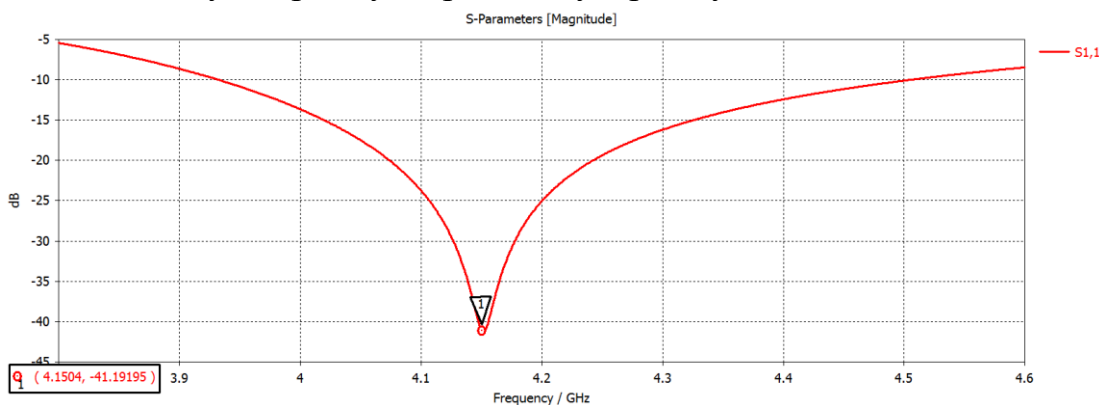


Рис.2. Частотна характеристика коефіцієнта відбиття S₁₁.

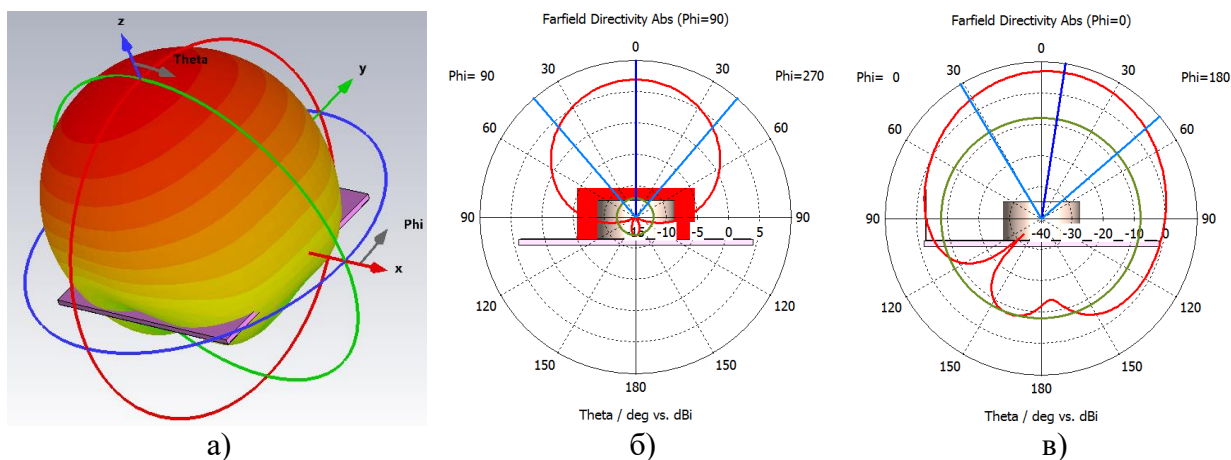


Рис.3. Діаграми спрямованості антени для частоти $f = 4,15$ ГГц.

Розрахункове значення коефіцієнту підсилення антени складає $G = 6,9$ дБі, ширина ДС у взаємно перпендикулярних площинах $2\varphi_{0,5} = 82^\circ$, $2\theta_{0,5} = 80^\circ$, найбільший рівень бічного випромінювання -15 дБ.

Таким чином, у даній роботі розкрито методику моделювання ДРА у програмному пакеті CST Studio Suite. Дана робота була підтримана Національним фондом досліджень України в рамках виконання грантового проєкту «Мікрохвильові пристрої на основі резонансних структур з метаматеріальним властивостями для захисту життєдіяльності та інформаційної безпеки України» (Реєстраційний номер проєкту 2021.01/0030) та НАТО в рамках виконання грантового проєкту NATO SPS G6002 "3D Metamaterials for Energy Harvesting and Electromagnetic Sensing".

Література

1. Ильченко М.Е. Электродинамика диэлектрических резонаторов / М.Е. Ильченко, А.А. Трубин. - К.: Наук. думка, 2004. — 264 с.
2. Aldo Petosa, Dielectric Resonator Antenna Handbook, Artech, 2007.
3. M. S. M. Aras, M. K. A. Rahim, A. Asrokin and M. Z. A. Abdul Aziz, "Dielectric resonator antenna (DRA) for wireless application," 2008 IEEE International RF and Microwave Conference, Kuala Lumpur, Malaysia, 2008, pp. 454-458, doi: 10.1109/RFM.2008.4897461.

ПОКРАЩЕННЯ ЕФЕКТИВНОСТІ СИМВОЛЬНОГО ПЛАНУВАННЯ В МЕРЕЖАХ 5G ШЛЯХОМ ЗАСТОСУВАННЯ СУМІСНИХ СЛОТОВИХ ФОРМАТІВ

Якорнов Є.А., Тичинський-Мартинюк В.Ю.

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна*

E-mail: yakornovits@gmail.com; tychynskyi-martyniuk.vitalii@lll.kpi.ua

IMPROVING THE EFFICIENCY OF SYMBOL - BASED SCHEDULING IN 5G NETWORKS BY USING COMPATIBLE SLOT FORMATS

Compatible formats and combinations of slot formats that are efficient with respect to criteria of minimum capacity and coverage loss are obtained. They can be recommended for dedicated and dynamic scheduling in synchronized 5G NR networks to reduce the effect of co-channel interference in border areas and interference between adjacent channels of operators at the national level.

З поточних опублікованих стандартів і досліджень були виявлені деякі помітні вразливості [1]. Ці вразливості 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, 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.

У даній доповіді розглянуто підходи до планування частотного і енергетичного ресурсів в синхронізованих мережах 5G NR на основі адаптації сумісних слотових форматів сигналу до умов застосування.

Вибір слотових форматів для дослідження

З метою прискорення визначення найбільш сумісних в мережах слотових форматів для дослідження із числа 62-х доступних форматів [2, р.135, Table 11.1.1-1], обираються ті, які найбільше відповідають динамічному характеру зміни заводового стану і трафіку в мережі за наступними критеріями:

- формати відповідають вимогам щодо динамічного вибору системою управління радіоресурсом (RRC), тобто формати можна віднести до групи «перехідних» із числа діючих. Решта форматів мають чіткі ознаки майже повної зміни попередніх форматів і є наперед несумісними за критеріями втрат ємності і покриття в разі обрання динамічного режиму зміни форматів;
- Збереження функціональності за призначенням (забезпечення сумісності базових станцій і планування мережі/мереж);
- максимальна ефективність (швидкість реакції, мінімальні ресурсні витрати на бланкування і на захисний інтервал на переходах DL-UL);

За цими критеріями для дослідження визначено 10 форматів (№№ 44 – 53).

Оцінка втрат ємності.

Методика оцінки втрат ємності ілюструється рис.1, де представлені формати слотів 45 і 47. Формат 45 містить 6 символів на передачу (DL), 6 гнучких символів (F) і 2 символи на прийом (UL). Формат 47 містить 2 символи на передачу, 2 гнучких символи і 10 символів на прийом. Втрати ємності можуть бути визначені шляхом обчислення уражених символів UL у слотовому форматі одного оператора через часове співпадіння із символами DL у слотовому форматі іншого оператора [3]. Для прикладу представлена модифікація 45А слотового формату 45, який застосовує один оператор, шляхом заміни у форматі слотів у гнучких символах на позиціях 8 і 22 на символи UL з урахування захисного інтервалу (позиції 7 і 21) між символами DL (позиції 6 і 20) і UL. Нижче представлена модифікація 47А формату 47, який застосовує другий оператор, шляхом заміни в форматі слотів гнучких символів на позиціях 3 і 10 на захисний інтервал.

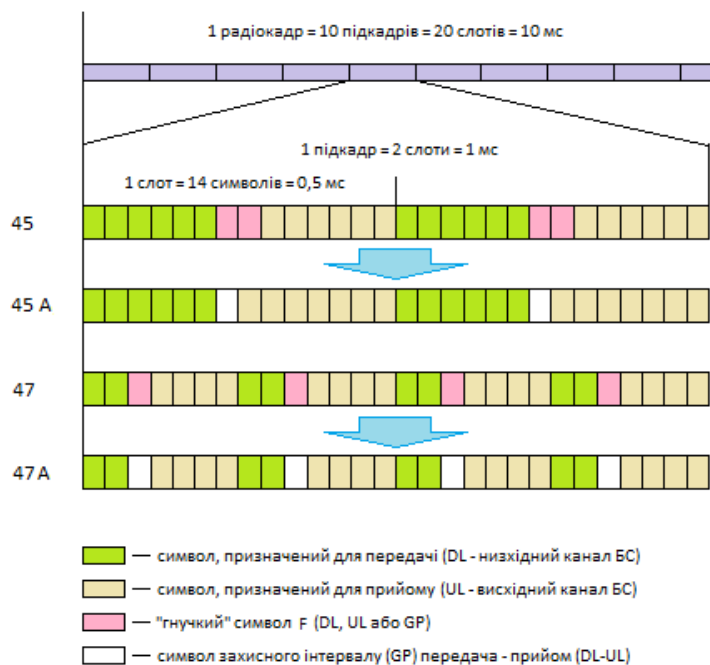


Рис.1. Модифікація слотових форматів шляхом заміни гнучких символів.

Втрати ємності у наведеній парі (45А і 47А) форматів становлять 55 %. Надалі шляхом заміни наступної позиції гнучкого символу на позиції 8 або 22 формату 45 на прийом (UL) отримаємо нову комбінацію взаємодії з форматом 47. Шляхом перебору всіх позицій гнучких символів для застосування DL, UL і GP (Guard Period) можна сформувати матрицю взаємодії для всіх можливих позицій гнучких символів у 10-ти слотових форматах, яка містить 135

комбінацій попарної взаємодії. Результати розрахунків втрат ємності для різних варіацій комбінацій форматів слотів 44-53 наведені на рис.2.

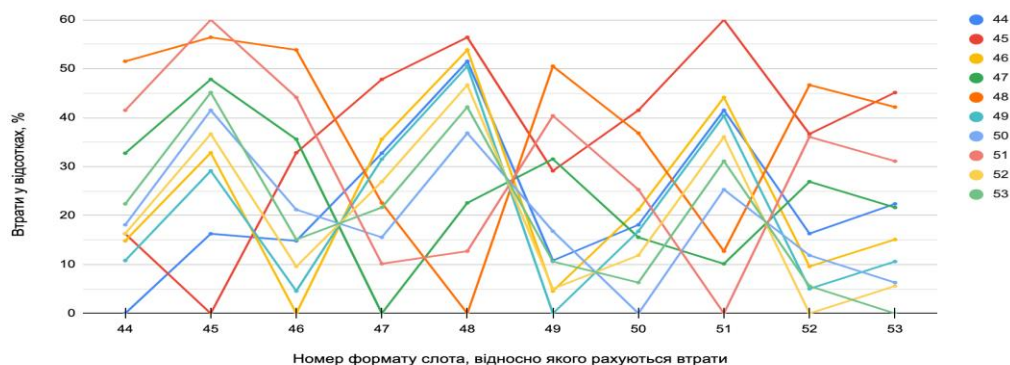


Рис.2. Втрати ємності (у %) в каналі UL в залежності від комбінацій форматів слотів 44 – 53.

При допустимих втратах ємності у 10% найкращі результати можна очікувати при застосуванні наступних 6-ти пар слотових форматів: 46-49; 46-52; 49-44; 49-52; 49-53; 52-53. При допустимих втратах ємності у 5% найкращими є 4 пари слотових форматів: 46-49; 46-52; 49-52; 52-53.

Оцінка втрат покриття.

Оцінка втрат покриття в слотових форматах здійснюється шляхом врахування енергетичних втрат на випромінювання в позиціях тих символів UL, які припадають на позиції символів блоку сигналу синхронізації (SSB - Synchronisation Signal Block). Перевагу будуть мати ті формати, в яких символні позиції DL співпадають з символними позиціями SSB (4 символи). Сигнали SSB в слотовому форматі мають фіксовані позиції, які визначаються стандартом [2, 4.1 Cell Search] і залежать від частотного діапазону і частотного рознесення піднесучих (SCS - **Sub Carrier Spacing**). Так, наприклад, для частотного діапазону 3ГГц (3,4-3,8 ГГц) і SCS у 30 кГц в радіокадрі розміщується 8 сигналів SSB у перших 4-х слотах, початкові позиції яких приходяться на символні позиції 4, 8, 16, 20, 32, 36, 44, 48. На рис.3 представлені модифіковані формати слотів 45А і 47А з позначеними місцями розміщення сигналів SSB. Розрахунок втрат покриття у радіокадрі для розміщення гнучких символів формату 47А становить 8,5 відсотків.

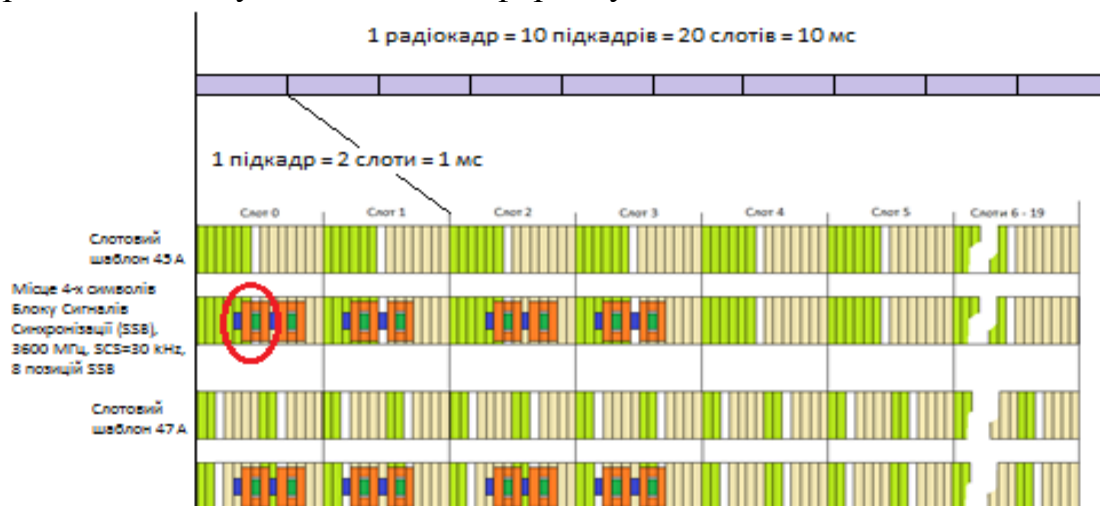


Рис. 3. Розташування сигналу SSB в форматі радіокадру.

Результати розрахунків для різних варіацій слотових форматів показують, що при допустимих втратах покриття у 5% кращі показники мають формати слотів 44, 46, 49, 52, що підтверджує кращу сумісність комбінацій цих форматів (плюс формат 53), отриманих за критерієм втрат ємності.

Література

1. Правило В.В. Аналіз потенційних вразливостей та загроз в 5G. //XVII Міжнародна науково-технічна конференція "Перспективи телекомунікацій" ПТ-2023: Збірник матеріалів конференції. К.: КПІ ім. Ігоря Сікорського, 2023. – с.33-35.
2. 3GPP TS 38.213 V17.2.0 (2022-07)/ETSI TS 138.213: "NR; Physical layer procedures for control", (2021-08), p.135, Table 11.1.1-1
3. ECC Report 331: Efficient usage of the spectrum at the border of CEPT countries between TDD MFCN in the frequency band 3400-3800 MHz, November 2021, www.cept.org

ANALYSIS OF THE CHARACTERISTICS OF ROUTING PROTOCOLS IN AD-HOC NETWORK

Astrakhantsev A.A., Hryschuk I.A., Pedan S.I.

Educational and Scientific Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: aastrakhantsev@its.kpi.ua,

hryschuk.iryana@gmail.com, stas.pedan@gmail.com.

ДОСЛІДЖЕННЯ ХАРАКТЕРИСТИК ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ В АД-НОС МЕРЕЖІ

Adhoc мережі набувають значного поширення останнім часом. Впровадження 5G є одним із чинників які прискорюють цей процес. Але стрімкий зріст окрім переваг має і ряд обмежуючих чинників. Одним із таких чинників є велика кількість існуючих протоколів маршрутизації і відсутність стандартизації вже цьому питанні. Тому ця робота присвячена дослідженню ефективності протоколів маршрутизації в adhoc мережах при різних зовнішніх параметрах, таких як рівень навантаження чи мобільність користувачів. Результати дослідження дозволяють обрати найкращий алгоритм маршрутизації в залежності від заданих умов.

Researching the characteristics of routing protocols in ad-hoc networks is a highly relevant task in telecommunications, as wireless ad-hoc networks are becoming increasingly prevalent in remote regions, even in extreme conditions, military operations, and scenarios where establishing infrastructure networks is not feasible. Routing protocols are essential for ad-hoc networks to ensure efficient and reliable data exchange between network nodes. However, due to such networks' dynamic and unpredictable nature, selecting the optimal routing protocol becomes challenging. Current research in this area is necessary to optimize the operation of ad-hoc networks and ensure their best functioning.

Analyzing the characteristics of different protocols enables telecommunications engineers to understand their advantages and limitations, thereby facilitating the development of optimal solutions to enhance the functionality and efficiency of ad-hoc networks in various application scenarios. Current challenges include high variability in packet loss, network instability when users' movement speed changes, and insufficient efficiency of routing protocols in ad-hoc networks.

This work aims to analyze the dependency of packet loss on network uptime, study the impact of users' movement speed on network efficiency, and investigate the effectiveness of different routing protocols in network operation. To achieve this goal, simulations were conducted to collect and analyze relevant information regarding network dynamics, users' movement speeds, and the selected routing protocol. We commenced the research by choosing the optimal moment for simulation to ensure the stability of the metrics. We considered various user movement patterns to identify robust metrics. The research results are presented in a graph, enabling the selection of the best time for further analysis. To thoroughly study packet behavior over different periods, we plan to conduct eight simulations ranging from 70 to 50,000 seconds. These data will be the basis for developing optimization strategies and network management to improve productivity and efficiency (Figure 1).

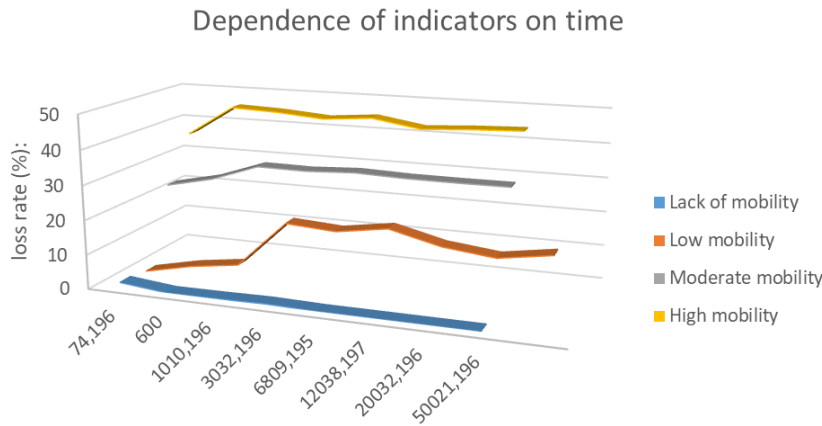


Fig. 1. Dependence of indicators on time.

During the initial stages of network operation, there is a notable exponential growth in traffic, leading to system instability. Conducting research on network parameters during such periods becomes impractical due to the need for more stability to ensure reliable results.

Therefore, waiting for the network to enter a stable operational mode for the load to stabilize and reach its maximum

values before embarking on scientific research and network analysis is advisable.

Accordingly, the optimal time interval for conducting research is 20,000 seconds or more. Only under such conditions can sufficient stability and reliability of the obtained data be ensured for further analysis and practical application.

In the subsequent stage of the study, the impact of user mobility on the efficiency of ad-hoc networks using the AODV protocol was analyzed (see Table 1). Notably, for this study, two fixed communication nodes were established, interacting with mobile nodes of varying velocities.

Table 1. Analyzing the impact of user speed on network efficiency.

Speed	loss rate (%):	round-trip avg (ms):	stddev (ms):
Lack of mobility	0,00297965	1.91593	0,101542
Low mobility	16.0342	177,603	857,769
Moderate mobility	30,7564	460,749	1255,67
Fast mobility	43,6678	787,03	1521,98

From the perspective of a telecommunications engineer, the research findings indicate that as the user speed in an ad-hoc network using the AODV protocol increases, data loss increases, as does the average connection setup time and its standard deviation.

In cases where user movement speed is low or mobility is absent, the network efficiency is relatively high, as evidenced by minimal data loss and low average connection setup time. Such conditions may be typical for stationary or low-mobility objects, such as sensors in monitoring systems.

However, in cases where user movement speed is high (moderate to high mobility), network efficiency significantly deteriorates, leading to significant data loss and increased connection setup time. Such conditions may arise, for example, in mobile applications or scenarios where users move quickly.

Thus, an ad-hoc network using the AODV protocol may be effective when a fast and reliable connection between nodes is required in cases of low or zero mobility. However, issues with network stability and efficiency may arise in cases of high mobility, necessitating additional optimization measures or the selection of a different network type.

In the final stage of the study, an evaluation of network performance using different routing protocols, including AODV, DSDV, and GPSR, was conducted (see Table 2). The results provided important information regarding the performance of each protocol under different network conditions. Specifically, the AODV and GPSR protocols demonstrated low levels of data loss and small average delay times, highlighting their high efficiency in route establishment and data exchange in the network. On the other hand, the DSDV protocol showed significant data loss and ample average delay time, indicating its lesser efficiency than other protocols.

Table 2. Investigation of network performance under different routing protocols.

Протокол	loss rate (%):	round-trip avg (ms):	sent
AODV-1	0.00595752	3.15598	33571
AODV-M	0.00596303	4.81104	33540
DSDV	7,99487	13,9246	33559
GPSR-M	0,152103	14,2624	33530
GPSR-M	0,149134	14,2303	33527

Conclusion. The conducted research confirms the relevance of analyzing routing protocol characteristics in ad-hoc networks, especially considering their prevalence in remote regions and conditions where establishing infrastructure networks is not feasible.

The research results underscore the importance of selecting the optimal routing protocol depending on specific application conditions, such as user mobility and network stability. High user mobility rates may lead to significant data losses and network efficiency degradation, necessitating careful protocol selection and potential optimization strategies.

References

1. Gobindgarh, M. N. Hoda, Umang Singh, Milind, Parul Choudhary. "Simulation of AODV, DSR and DSDV Routing Protocols for Mobile Ad-hoc Networks." Proceedings of the 2nd National Conference on "Challenges and opportunities in IT", RIMT-Institute of Engineering and Technology, Mandi Gobindgarh, March 29, 2008.
2. Pradeep Kumar T S. "Real-Time Traffic Simulation of Vehicular Ad hoc Networks." Chapter in "VIT University Chennai", September 2022.
3. Pestin, Maxim S., Novikov, Alexander S. "Simulation model of wireless ad-hoc network to study algorithms of traffic routing." Journal of Applied Informatics, August 2022, Vol. 17, Issue 4, pp. 75-86. DOI: 10.37791/2687-0649-2022-17-4-75-86.
4. Augustine Chidiebere Onuora, Chiemezuo Njoku Festus O Ogbunude, Osu Moses. "A Comparative Study of Simulation Tools for Ad hoc Networks." Proceedings of the Conference on Evaluating the Policies and funding for engineering sustenance: A panacea for functional Engineering product for economic emancipation, AIFPU, Ebonyi State, Nigeria, June 2021.

ОПТИМІЗАЦІЙНИЙ ПІДХІД ДО ВИБОРУ ПАРАМЕТРІВ МІКРОХВИЛЬОВИХ ЛІНІЙ ЗВ'ЯЗКУ ПРЯМОЇ ВИДИМОСТІ

Лагода А.В., Трубаров. І.В.

Інститут телекомунікаційних систем

КПІ ім. Ігоря Сікорського, Україна

E-mail: anastasialahoda@gmail.com

OPTIMIZATION APPROACH FOR SELECTION OF MICROWAVE LINE-OF-SIGHT LINK PARAMETERS

The ITU recommends using a specific algorithm to determine antenna heights, emphasizing the importance of optimizing the clearances above the height of the antenna itself.

In our methodology, we have improved this approach to include the calculation of optimal antenna heights and diameters. We introduce a procedure that allows us to find such antenna heights and diameters that are minimal in terms of equipment cost, antenna diameter, and mast length, but still provide high signal quality.

Мікрохвильові лінії прямої видимості складаються з систем "точка-точка" між двома наземними станціями, які передають і приймають сигнали, використовуючи переваги поширення хвиль через нижню частину атмосфери (тропосферу). Мікрохвильові лінії працюють в режимі прямої видимості в діапазонах частот від 400 МГц до 95 ГГц за певних умов доступності та якості. На практиці ці системи називають мікрохвильовими лініями зв'язку, мікрохвильовими лініями прямої видимості, радіолініями фіксованої служби або просто радіолініями.

Шлях поширення хвильового фронту між передавачем і приймачем мікрохвильової лінії прямої видимості є вигнутою траєкторією. Якщо проаналізувати радіогоризонт (відстань, на якій хвильовий фронт перехоплює кривизну Землі), то виявиться, що ця відстань може бути як більшою, так і меншою за геометричну відстань до оптичного горизонту (дотична до Землі, що проходить повз передавач), залежно від умов тропосфери, що можна побачити на рис.1.

Загальна методика визначення висот підвісу антен полягає в тому, що ITU рекомендує [2] визначати антени виходячи з критерію забезпечення необхідного просвіту, але вона не визначає конкретних оптимальних значень висот машт польоту. Пропонується включити три параметри: діаметр антени (передбачається, що антени на обох кінцях польоту однакові), висота підвісу, антени передавача та висота підвісу антени приймача, в структуру оптимізації. Також потрібно визначити такі параметри за яких виконуються параметри якості: Клас 4 за рекомендацією ITU-R F.696-2[3] при якому ESR = 0.4% та відсоток часу загальної неготовності польоту (P_u) є 0.1%. При цьому нашою метою є досягнення мінімальної загальної вартості обладнання. Для цього необхідно ввести моделі вартості які можуть бути будь-якими та у

якості методу оптимізації обирається метод повного перебору варіантів.

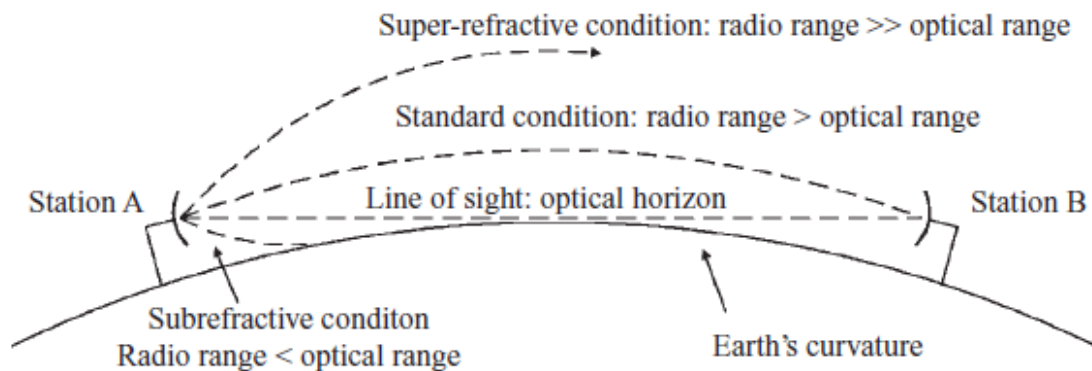


Рис. 1. Оптичний горизонт та радіогоризонт [1].

Метод перебору варіантів вважається найбільш точним серед усіх методів оптимізації, оскільки він гарантує знаходження істинного оптимуму. Однак його недолік полягає у великій обчислювальній складності: при великій кількості параметрів обчислення може займати значний час, або навіть стати неможливим у зв'язку з необхідністю провести повний перебір, що може зайняти надзвичайно багато часу або навіть вимагати нескінченного часу для завершення.

Однак у випадку описаної задачі, де кількість номіналів діаметрів антен та кількість секцій машт відносно невелика - 10 номіналів антен та 15 секцій машт, загальна кількість варіантів перебору становить 2250. Така кількість варіантів є прийнятною для використання методу перебору варіантів без значного збільшення часу обчислень. Отже, в рамках перевірки підходу, що пропонується, було здійснено моделювання та оптимізацію радіорелейної лінії зв'язку з параметрами, наведеними в табл. 1. Сама графічна діаграма радіорелейного прольоту за результатами оптимізації на рис. 2.

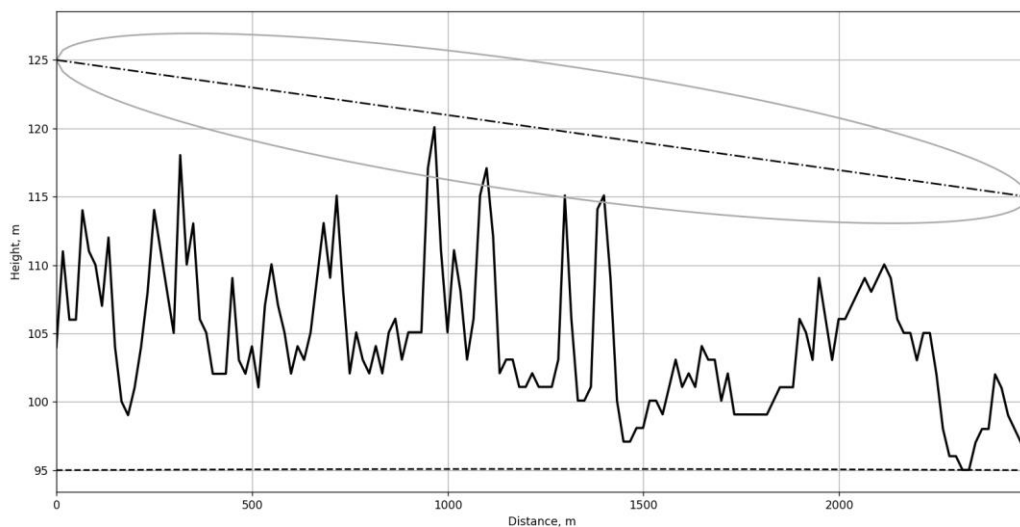


Рис.2. Графічна діаграма радіорелейного прольоту

Табл. 1. Параметрами ліній.

Відсоток недоступності через багатопроменеве поширення хвиль, %	0.0002
Частота, МГц	8000
Потужність передавача, дБм	20.0
Чутливість приймача, дБм	-66
Коефіцієнт підсилення антени, дБ	25.404
Відстань зв'язку, м	2481.468
Оптимальний діаметр антени	0.3 m
Оптимальна висота антени з боку передавача	21.0 m
Оптимальна висота антени з боку приймача	18.0 m
Оптимальне значення загальної вартості обладнання радіорелейної лінії, відносні одиниці	235485.568
Оптимальне значення проясвітту	1.021 m

В роботі реалізовано таку задачу оптимізації і знайдено такі висоти підвісу антен і діаметри антен, щоб загальна вартість цього обладнання була найменшою, діаметри антен були найменшими, сумарна довжина машт підвісу також була найменшою, але при цьому усі показники якості виконувалися за допомогою методу перебору варіантів.

Даний метод виправданий оскільки дуже швидко дозволяє обрати оптимальні параметри і при цьому він не залежить від конкретних моделей вартості обладнання. Тобто воно може задаватись різними способами.

Література

1. Pablo Angueira, Juan Antonio Romo / Microwave line of sight link engineering.
2. ITU-R P.530 Propagation data and prediction methods required for the design of terrestrial line-of-sight systems (09/2021).
3. ITU-R F.696-2 Error performance and availability objectives for hypothetical reference digital sections forming part or all of the medium-grade portion of an integrated services digital network connection at a bit rate below the primary rate utilizing digital radio-relay systems (02/1997).

ЗАБЕЗПЕЧЕННЯ ЗАДАНИХ ПОКАЗНИКІВ БЕЗПЕКИ ПЕРЕДАЧІ ДАНИХ В 4G МЕРЕЖАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Правило В.В.

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

ENSURING THE SPECIFIED SECURITY INDICATORS OF DATA TRANSMISSION IN 4G NETWORKS OF SPECIAL PURPOSE

A set of measures is being considered to ensure a given level of data transmission security in 4G networks. Possible ways of unauthorized access by attackers to the network were analyzed. Directions for ensuring the security of special purpose 4G networks are proposed.

Сучасні військові операції вимагають високої мобільності, ефективності та безпеки. Для забезпечення цих вимог Збройні Сили України активно впроваджують нові технології, в тому числі 4G мережі.

4G мережі дозволяють військовим залишатися на зв'язку один з одним, навіть якщо вони знаходяться в русі. Вони також забезпечують більш високу швидкість передачі даних, що важливо для координації дій та управління технікою.

Для забезпечення заданого рівня безпеки передачі даних в 4G мережах необхідно використовувати комплекс заходів, включаючи шифрування, аутентифікацію та авторизацію.

Забезпечення заданого рівня безпеки передачі даних в 4G мережах передбачає використання наступних заходів:

- Застосування шифрування з відкритим ключем для аутентифікації та авторизації пристроїв. Це дозволяє забезпечити більш надійну ідентифікацію пристроїв і користувачів.

- Використання криптографії з симетричним ключем для захисту даних від несанкціонованого доступу. Це дозволяє забезпечити більш надійне шифрування даних.

- Використання технології SDN для управління мережею та виявлення атак. Це дозволяє швидко і ефективно виявляти та реагувати на атаки.

4G мережі використовують протоколи аутентифікації та авторизації, які можуть бути вразливими до атак. Це означає, що зловмисники можуть отримати доступ до мережі, використовуючи підроблені ідентифікатори. Вони не забезпечують достатнього захисту від атак на рівні даних. Це означає, що зловмисники можуть отримати доступ до даних, навіть якщо вони не зможуть отримати доступ до мережі. Для забезпечення заданого рівня безпеки передачі даних 4G мережах необхідно використовувати комплекс заходів, включаючи криптографію, аутентифікацію та авторизацію.

Криптографія використовується для захисту даних від несанкціонованого доступу. Криптографія використовує математичні алгоритми для перетворення даних в нечитабельний формат, який можна розшифрувати лише за допомогою правильного ключа.

Для шифрування даних, що передаються в 4G мережах, доцільно використовувати алгоритми шифрування ERCA та EPS (EEA).

ERCA – це алгоритм симетричного шифрування, який використовує ключі довжиною 256 біт. Він заснований на алгоритмі Rijndael, який є одним із найбезпечніших алгоритмів симетричного шифрування, доступних на сьогодні.

EPS (EEA) – це алгоритм асиметричного шифрування, який використовує ключі довжиною 128 біт. Він є алгоритмом відкритого ключа, що означає, що існують два ключі: приватний ключ і відкритий ключ. Приватний ключ використовується для шифрування даних, а відкритий ключ використовується для дешифрування даних.

В таблиці 1 представлені основні відмінності між алгоритмами ERCA і EPS.

Таблиця 1. Основні відмінності між алгоритмами ERCA і EPS.

Характеристика	ERCA	EPS
Тип шифрування	Блочний	Пакетний
Довжина ключа	256 біт	128 біт
Дані, які захищаються	Голосові дзвінки, текстові повідомлення, дані передачі даних	Сигнали управління мережею, дані, які передаються між базовими станціями

Аутентифікація використовується для перевірки ідентифікаторів пристроїв та користувачів. Аутентифікація допомагає гарантувати, що лише авторизовані пристрої та користувачі можуть отримати доступ до мережі.

Авторизація використовується для визначення того, що пристрої та користувачі можуть робити в мережі. Авторизація допомагає гарантувати, що лише авторизовані пристрої та користувачі можуть отримувати доступ до певних ресурсів або виконувати певні дії.

Поточна система безпеки 4G/LTE не визначає наскрізну архітектуру безпеки, яка може забезпечити безпечні сеанси для двох UE, підключених до двох різних мереж LTE.

Для вирішення цієї проблеми пропонується використовувати пакетний ключ, час життя якого зводиться до пакетного періоду.

Це дослідження спрямоване на вдосконалення локальної системи безпеки 4G/LTE, подальше розширення наскрізної системи безпеки для захисту даних користувачів між різнорідними мережами доступу LTE. Цей

процес, за допомогою якого кожна пара UE всюди отримує свій KASME, подібний до процесу 4G/LTE (рис.1) .

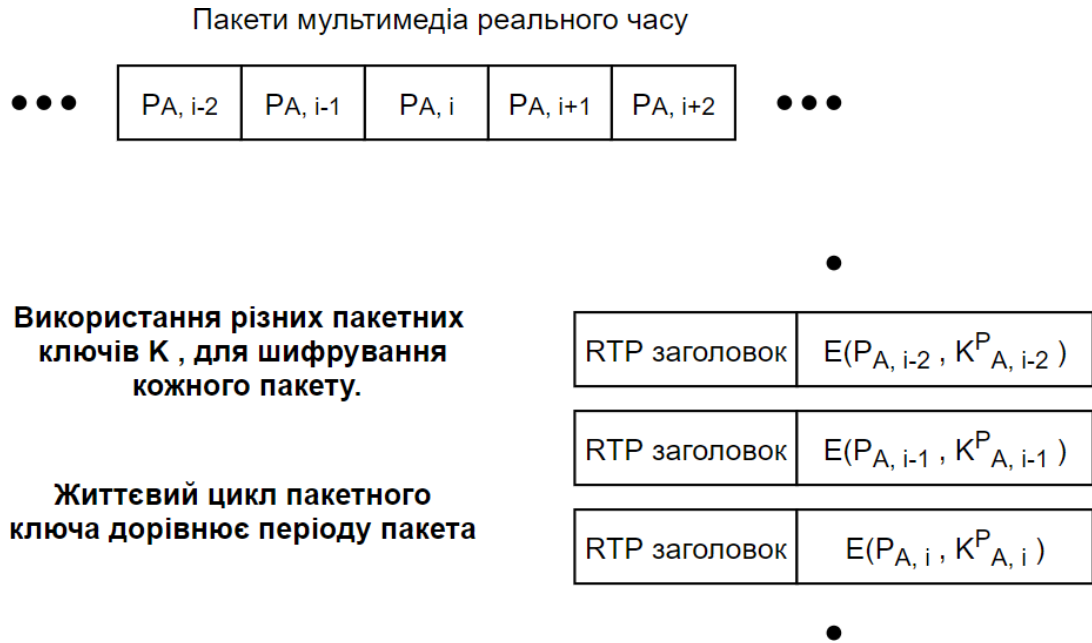


Рис. 1. Використання ключів пакетів для захисту потоку пакетів.

Аутентифікація в рамках забезпечення заданого рівня безпеки передачі даних в 4G мережах використовується для перевірки ідентифікаторів пристроїв та користувачів. Це допомагає гарантувати, що лише авторизовані пристрої та користувачі можуть отримати доступ до мережі.

Авторизація в рамках забезпечення заданого рівня безпеки передачі даних в 4G мережах використовується для визначення того, що пристрої та користувачі можуть робити в мережі. Це допомагає гарантувати, що лише авторизовані пристрої та користувачі можуть отримувати доступ до певних ресурсів або виконувати певні дії.

Таким чином пропонується забезпечення заданого рівня безпеки передачі даних в 4G мережах за допомогою схеми впровадження ключа пакетів. Дане рішення збільшує рівень безпеки при передачі, а також після перехоплення зломисником потоку пакетів.

Література

1. 3GPP TR 25.814 Physical layer aspects for evolved Universal Terrestrial, Radio Access (UTRA), Release 7), V7.1.0, 2006. pp.64
2. G.-H. Tu, C.-Y. Li, C. Peng, Y. Li and S. Lu, "New security threats caused by IMS-based SMS service in 4G LTE networks".
3. J. Henrydoss and T. Boulton, "Critical security review and study of DDoS attacks on LTE mobile network".
4. R. P. Jover, J. Lackey and A. Raghavan, "Enhancing the security of LTE networks against jamming attacks", EURASIP J. Inf. Secur.

ВИБІР ОПТИМАЛЬНИХ ПАРАМЕТРІВ ЛЧМ СИГНАЛУ ДЛЯ КАНАЛІВ ЗВ'ЯЗКУ БПЛА, РЕАЛІЗОВАНИХ НА БАЗІ SDR ТРАНСІВЕРІВ

Кайденко М.М., Роскошний Д.В.

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна
E-mail: kkk610@ukr.net*

SELECTION OF OPTIMAL CHIRP SIGNAL PARAMETERS FOR UAV COMMUNICATION CHANNELS IMPLEMENTED ON THE BASIS OF SDR TRANSCEIVERS

This article discusses the possibility of using CSS modulation for UAV communication channels. Methods for forming chirps on FPGAs, as well as their parameters when used in SDR transceivers, have been studied. The results of experimental studies using the AD9364 SDR transceiver of the spectral characteristics of CSS sequences are presented.

Захист каналів зв'язку безпілотних літальних апаратів (БПЛА) від впливу на них навмисних завад стає все більш актуальною задачею. В роботі [1] визначені усі типи завад, які можуть впливати на канали зв'язку БПЛА. Найбільш вразливими канали зв'язку є до енергетичних завад, особливо це стосується малогабаритних БПЛА внаслідок того, що для них не завжди можна використати ефективні методи протидії різним видам завад, запропонованим в роботі [2]. Проста широкопasmовою завада легко створюється і ефективно діє в зоні виконання місії БПЛА, в цьому полягає її шкідливість та необхідність ефективно їй протидіяти. Наряду з застосуванням запропонованих методів протидії навмисним завадам необхідно використовувати такі методи протидії, як використання сигналів з розширенням спектру, що зменшить вплив енергетичних завад на канали управління та телеметрії, підвищуючи живучість БПЛА.

Існують наступні методи розширення спектру: стрибків робочої частоти - FHSS (Frequency Hopping Spread Spectrum); прямої послідовності - DSSS (Direct Sequence Spread Spectrum); лінійної частотної модуляції - CSS (Chirp Spread Spectrum); часових стрибків - THSS (Time Hopping Spread Spectrum); гібридні поєднання попередніх методів (Hybrid Spread Spectrum).

Останнім часом все більше уваги приділяється застосуванню CSS модуляції, яке стало можливим з розвитком елементної бази цифрової обробки сигналів. Як і в інших методах розширення спектру, CSS використовує всю виділену смугу пропускання для передачі сигналу, що робить його стійким до каналних шумів. Крім того, оскільки ЛЧМ-сигнали використовують широку смугу спектру, CSS також стійкий до багатопроменевого завмирання навіть при роботі на дуже низькій потужності. Однак він відрізняється від розширеного FHSS та DSSS тим, що він не додає жодних псевдовипадкових елементів до сигналу, щоб допомогти відрізнити його від шуму в каналі, замість цього покладаючись на лінійний характер ЛЧМ-імпульсу. Окрім того, що також важливо, CSS стійкий до впливу ефекту Доплера, що є типовим для мобільних

систем зв'язку. Недоліком CSS є складність реалізації.

Дана робота присвячена опису результатів дослідження можливостей реалізації CSS на базі SDR трансивера.

Можливі два методи формування ЛЧМ сигналу на SoC (FPGA): генератор, базований на використанні записаних в пам'яті відліків сигналу (Memory-based Chirp Cenerator) та генератор з використанням прямого синтезу частоти (Direct Digital Synthesizer (DDS) Chirp Cenerator) [3]. Обидва методи мають свої недоліки та переваги. Не зважаючи на гірший рівень викривлень сигналу для телекомунікаційних застосувань реалізація на базі SDR трансиверу варіанту Memory-based Chirp Cenerator є більш прийнятною внаслідок того, що таким чином істотно спрощується маніпуляція при переході від одного стану (UP-Chirp) до іншого (Down-Chirp) та можливість застосування багатопозиційних видів маніпуляції, як приклад рекомендованих в [4] та використаних в технології LoRa [5].

Формування ЛЧМ сигналу на SDR трансивері здійснюється в основній смузі частот, також можливе застосування квадратурної модуляції, що дозволяє істотно спростити подальшу обробку сигналу в приймачі.

В загальному вигляді ЛЧМ -імпульс описується як:

$$s(t) = \cos(2\pi(f_0 t + \frac{\alpha}{2} t^2)) \quad (1)$$

де: $\alpha = B/T = (f_1 - f_0)/T$, T-тривалість ЛЧМ-імпульсу.

При створенні ЛЧМ імпульсу в основній смузі частот $\alpha = B/T = (f_{max} - f_{min})/T$, при цьому f_{max} та f_{min} відповідно максимальна та мінімальна частоти імпульсу не залежно від того, яким чином він формується: зі збільшенням частоти UP-Chirp чи зі зменшенням Down-Chirp.

При дискретному представленні ЛЧМ-імпульсу, він описується як:

$$s[n] = \cos(2\pi[f_0 n + \frac{\alpha}{2(N-1)} n^2]) \quad (2)$$

Використання квадратурної модуляції дозволяє представити та створити квадратурний ЛЧМ-імпульс:

$$s[n] = \cos(2\pi[f_0 n + \frac{\alpha}{2(N-1)} n^2]) + i \sin(2\pi[f_0 n + \frac{\alpha}{2(N-1)} n^2]) \quad (3)$$

Верхня частота сигналу визначається максимальною частотою дискретизації ЦАП SDR трансиверу та необхідною кількістю відліків на період максимальної частоти ЛЧМ імпульсу. Для AD9361 (AD9364) - $f_{sample} = 61,44$ МГц (при цьому частота дискретизації може бути збільшена до 122,88МГц шляхом виключення напівсмугових фільтрів в трактах передачі чи прийому). З другої сторони верхня частота обмежується смугою пропускання SDR трансивера, для AD9361 смуга пропускання 56 МГц (± 28 МГц відносно центральної частоти налаштування передавача). Кількість відліків на період максимальної частоти може бути вибрана мінімально можливою ($n=2$ відліки), при цьому формування сигналу на вході цифро-аналогового перетворювача та зниження міжсимвольної інтерференції забезпечується використанням каскаду фільтрів інтерполяторів та багатофазного КІХ-фільтру з сумарним коефіцієнтом

інтерполяції до 11 SDR трансивера. Нижня частота визначається необхідною смугою частот ЛЧМ сигналу, при цьому слід враховувати оптимальну різницю в кількості відліків на період між верхньою частотою та нижньою.

Важливим параметром є тривалість ЛЧМ імпульсу, оскільки вона визначає базу сигналу та каналну швидкість передачі інформації. Окрім того при дискретному представленні сигналу довжина повинна бути кратна періоду дискретизації та співвідноситись як N/f_{sample} . При цьому N повинно бути кратне ступеню 2 для того, щоб при обробці сигналу не виникало необхідності доповнювати послідовність нулями.

На рис. 1 представлено результати експериментальних досліджень спектрів сформованих псевдовипадкових послідовностей ЛЧМ-імпульсів, які були передані, а потім прийняті з використанням SDR трансиверу AD9364 (Pluto SDR) в режимі DAC Buffer Output для наступних умов: Частота дискретизації $f_{\text{sample}} = 61,44$ МГц, кількість відліків $N=1024$, тривалість ЛЧМ-імпульсу $T_{\text{chirp}} = 167$ мксек з використання багатозафазного КІХ-фільтру. На рис.1 а) — максимально можлива з точки зору частоти дискретизації смуга робочих частот ($f_{\text{max}} = f_{\text{sample}}/2$), на рис.1 б) — оптимальна смуга робочих частот 20 МГц.

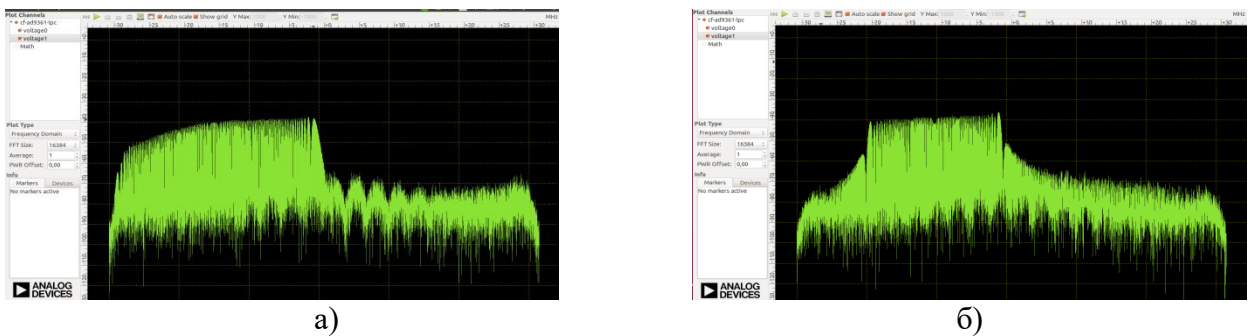


Рис.1. Спектр псевдовипадкової послідовності ЛЧМ-імпульсів для різних смуг частот переданих ра прийнятих SDR трансивером AD9364.

Література

1. 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>.
2. 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
3. Chua Ming Yam, and Voon Koo, "FPGA-Based Chirp Generator for High Resolution UAV SAR," Progress In Electromagnetics Research, Vol. 99, 71-88, 2009. doi:10.2528/PIER09100301.
4. "IEEE Standard for Low-Rate Wireless Networks," in IEEE Std 802.15.4-2020 (Revision of IEEE Std 802.15.4-2015) , vol., no., pp.1-800, 23 July 2020, doi: 10.1109/IEEESTD.2020.9144691.
5. Noor-A-Rahim, M.; Khyam, M.O.; Mahmud, A.; Li, X.; Pesch, D.; Poor, H.V. Hybrid Chirp Signal Design for Improved Long-Range (LoRa) Communications. Signals 2022, 3, 1-10. <https://doi.org/10.3390/signals3010001>.

РЕАЛІЗАЦІЯ УЗГОДЖЕНОГО ФІЛЬТРУ ДЛЯ ЛЧМ СИГНАЛІВ ПРИ ВИКОРИСТАННІ SDR ТРАНСИВЕРА НА БАЗІ SYSTEM-ON-CHIP

Кайденко М.М., Роскошний Д.В.

*Навчально-науковий інститут телекомунікаційних систем КІІ ім. Ігоря Сікорського, Україна
E-mail: ккк610@ukrl.net*

IMPLEMENTATION OF A MATCHED FILTER FOR LFM SIGNALS USING A SYSTEM-ON-CHIP BASED SDR TRANSCEIVER

The use of LFM signals in UAV communication channels is gaining more and more popularity. The main problem of using LFM for data transmission is the implementation of matched filters. The article deals with the implementation in FPGA of a matched filter for LFM signal based on Fourier transform

Програмно визначені радіосистеми (SDR) - це системи радіозв'язку, де компоненти, які традиційно впроваджуються в апаратне забезпечення замість цього реалізуються за допомогою вбудованих систем, в яких обчислювальні елементи побудовані на сучасних пристроях обробки сигналів, таких як цифрові сигнальні процесори (DSP), програмовані логічні інтегральні схеми (FPGA), системи-на-кристалі (System-on-Chip або SoC) та ін.

Основна ідея використання пристроїв SDR полягає в тому, що одним або декількома аспектами функціональності радіопристрою можна керувати за допомогою програмного забезпечення.[1-3]

Особливий інтерес викликає вивчення можливостей застосування технології SDR при побудові каналів зв'язку з безпілотними літальними апаратами (БПЛА), оскільки вона дозволяє лише програмним способом забезпечити баланс вимог до швидкості та надійності передачі даних на необхідну відстань.

Узагальнена схема побудови SDR трансивера з використанням технологій System-on-Chip та SDR наведена на рисунку 1.

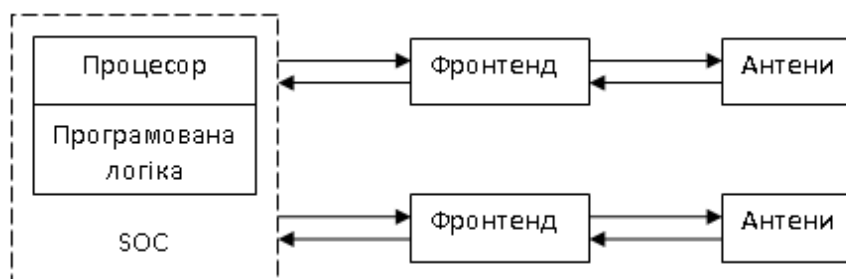


Рис. 1. Узагальнена схема побудови SDR трансивера.

При такому варіанті побудови трансивера фронтенд виконує функції формування сигналу (включаючи підсилювачі та фільтри), аналогового змішування та перетворення даних за допомогою АЦП та ЦАП, а безпосередня обробка сигналів виконується в системі на кристалі, до складу якої входять процесорний модуль та програмована логіка. Застосування такого підходу до побудови сучасних засобів зв'язку дозволяє суттєво розширити їх функціонал за рахунок можливостей цифрової обробки сигналів.

Останнім часом все більшої популярності набуває застосування ЛЧМ сигналів для передачі інформації, зокрема в каналах зв'язку БПЛА. Основною проблемою застосування ЛЧМ для передачі даних є реалізація узгоджених фільтрів. Це пов'язано з тим, що на сучасному етапі засоби зв'язку все більше “цифровізуються” і узгоджена фільтрація ЛЧМ сигналів здійснюється в цифровому вигляді на базі пристроїв ЦОС.

Узгоджена фільтрація є процесом виявлення відомого сигналу, спотвореного впливом шуму, тобто виконується операція кореляції між прийнятим сигналом та його відомим образом. На виході узгодженого фільтра ми отримуємо стиснений сигнал, тобто узгоджений фільтр використовується в якості фільтра стискання імпульсів, що забезпечує високе співвідношення сигнал/шум на його виході. Імпульсна характеристика узгодженого фільтра є оберненою в часі та спряженою копією образу переданого сигналу.

Одним з варіантів побудови узгоджених фільтрів є застосування прямого (ШПФ) та зворотного перетворення Фур'є (ЗШПФ). [5,6] В цьому випадку виконується перетворення Фур'є над сигналом та його образом (перехід з часової до частотної форми), після цього виконується перемноження Фур'є-образів та зворотне перетворення Фур'є (перехід з частотної до часової форми) цього добутку. Після цієї процедури при наявності в прийнятій суміші сигналу та шуму ми отримуємо короткий стиснений імпульс. Спрощена схема такого узгодженого фільтра наведена на рис 2.

Дослідження узгодженого фільтра були проведені з використанням стенду, побудованого за схемою, що наведена на рис 1. В якості фронтенда використана мікросхема AD9361, система на кристалі – на базі Cyclone V SX SoC—5CSXFC6D6F31C6N. [7]

При проведенні досліджень використовувались ІР – ядра зі складу пакету Quartus Prime.

ІР – ядра були сконфігуровані для обчислення ШПФ в трьох режимах - 512, 1024 та 2048 точок, вхідні дані отримувались з 12-розрядних АЦП.

При використанні ІР – ядер існує можливість конфігурування не тільки розрядності та довжини перетворення, а і способу обробки вхідних даних – різновиди потокової (streaming) та пакетної (burst). Використання потокової

обробки в порівнянні з пакетною дозволяє досягнути більшої швидкості обробки даних.

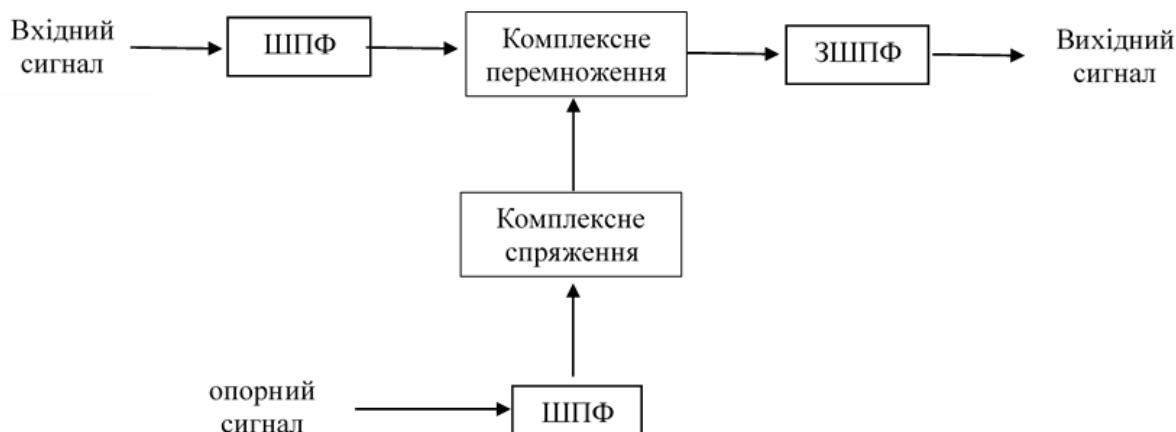


Рис. 2. Спрощена схема побудови узгодженого фільтра.

Опорний ЛЧМ сигнал для проведення досліджень був сформований наступним чином. В пам'яті FPGA була сформована ROM, в яку при ініціалізації записується 512 відліків, які відповідають чверті періода синусоїди.

Інші відліки формуються шляхом зміни знаку та/або напрямку зчитування даних.

Результати імплементації узгодженого фільтра наведено в таблиці 1

Таблиця .1 Результати імплементації узгодженого фільтра.

Кількість точок	Затримка, тактів	Використано логічних елементів	Використано перемножувачів
512	1040	12645	18
1024	2064	14980	18
2048	4112	18690	36

Література

1. Markus Dillinger; Kambiz Madani; Nancy Alonistioti (2003). Software Defined Radio: Architectures, Systems and Functions. Wiley & Sons. p. xxxiii. ISBN 0-470-85164-3.
2. Software Defined Radio in Communications. In: Pchenko M., Uryvsky L., Globa L. (eds) Advances in Information and Communication Technologies. UKRMICO 2018. Lecture Notes in Electrical Engineering, vol 560. Springer, Cham DOI https://doi.org/10.1007/978-3-030-16770-7_11 Print ISBN 978-3-030-16769-1, ISSN 1876-1100.
3. Кайденко М.М, Роскошний Д.В. «Архітектура та вибір компонентів для застосувань SDR» // XII Міжнародна науково-технічна конференція "Проблеми телекомунікацій" ПТ-2018 Збірник матеріалів конференції.К.: КПІ ім. Ігоря Сікорського, 2018.– с.205-208 ISSN (print) 2663-502X, ISSN (online) 2664-3057.
4. G. Turin, "An introduction to matched filters," in *IRE Transactions on Information Theory*, vol. 6, no. 3, pp. 311-329, June 1960, doi: 10.1109/TIT.1960.1057571.
5. L. Brigham, "The fast Fourier transform and its applications", Prentice Hall, 1988.
6. R.G. Lyons, "Understanding digital signal processing", Prentice Hall, 4th edition, 2010.
7. Altera, "Cyclone V Device Handbook, Volume 1", July 2014.

МЕТОДИ РЕАЛІЗАЦІЇ ТЕХНОЛОГІЇ ПЕРЕДАЧІ ГОЛОСУ VONR У МЕРЕЖАХ 5G. ОПЦІЇ ДЛЯ ІСНУЮЧИХ ОПЕРАТОРІВ

Ветошко І.П., Кравчук С.О.

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна
E-mail: ivan.vetoshko@ukr.net , sakravchuk@ukr.net*

METHODS FOR IMPLEMENTING VONR VOICE TECHNOLOGY IN 5G NETWORKS. OPTIONS FOR EXISTING OPERATORS

In the course of the study, we considered methods of implementing VoNR voice transmission technology in 5G networks for existing operators. The choice of method depends on the priority and capabilities of the operator. Each of these methods should be carefully considered, taking into account both their advantages and disadvantages, to achieve a successful implementation of VoNR in 5G networks

У нинішніх умовах впровадження стандарту 5G в мобільних мережах створює нові можливості для швидкого та безперервного обміну даними, але все ще існують певні проблеми з якістю голосових послуг у таких мережах. Особливий інтерес викликає реалізація послуг передачі голосу по новому радіо (VoNR). Перехід на новий стандарт вимагає глибокого розуміння і вирішення низки технічних питань. Архітектурні особливості мереж 5G, такі як висока пропускна здатність і низька затримка, створюють унікальні виклики для ефективної інтеграції голосових послуг.

Існують різні варіанти реалізації VoNR у мережі. З цих варіантів деякі з них підійдуть для існуючого оператора, а деякі - будуть найкращими для нового оператора. У діючого оператора (або нового оператора) може не бути розгорнутої мережі 5G Core, 5G NR та IMS. Тоді найкращим і доступним вибором буде — розгортання мережі IMS, яка підтримує інтерфейси HTTP, разом із новим розгортанням 5G Core та 5G NR [1].

Існуючий оператор, який прагне надавати голосові послуги, зрештою повинен запровадити VoNR. Для цього оператор повинен мати наступні передумови:

- в мережі вузли LTE eNB оновлено до gNB і підключено до нового 5GC;
- розгорнуті та працюють базова мережа IMS та голосовий сервіс VoLTE;
- по всій мережі оператора доступне нове покриття 5GC і 5G NR.

Тоді, оператор може розглянути наступні три методи реалізації VoNR:

1) розгортання модуля управління даними користувачів UDM (Unified Data Management) в ядрі 5G, яке також підтримує функції HSS (Home Subscriber Server) для IMS;

2) розгортання функції IWF (InterWorking Function), яка перетворює повідомлення протоколу сигналізації Diameter на HTTP та інтегрує існуючу мережу IMS із новим 5GC;

3) оновлення існуючого вузла IMS для підтримки нових інтерфейсів на основі HTTP та підключення вузла до нових основних мережних функцій 5G.

Кожен із цих методів має свої переваги та недоліки. Їх вибір залежить від прийнятої для них пріоритетності [2].

Так, перший метод включає вузли з подвійною функціональністю для плавного та швидшого розгортання послуг 5G будь-яким оператором (рис. 1). Більшість постачальників розробили конвергентні програми, такі як UDM з HSS і PCF (Policy Control Function) з PCRF (Policy and Charging Rules Function). Це допомагає оператору підключити мережу IMS безпосередньо до нового 5GC без будь-яких змін у існуючій мережі IMS і з меншими додатковими витратами [3]. Але при цьому за допомогою DRA (Diameter Routing Agent) необхідно відпрацювати процедуру контролю, що повідомлення через Diameter, пов'язане з користувачами 5G, правильно (по відношенню до узгодження різних протоколів сигналізації) направляється до 5G UDM і PCF.

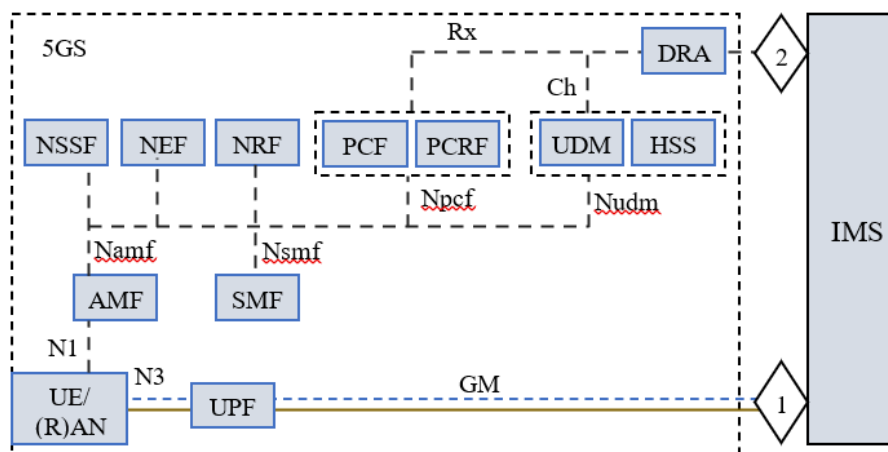


Рис. 1. Метод розгортання модуля управління даними користувачів UDM: (R)AN ((Radio) Access Network) – функція мережного доступу (радіодоступ, як одна з опцій); AMF (Access and Mobility Management Function) - функція управління доступом і мобільністю; SMF (Session Management Function) - функція управління сеансом; UE (User Equipment) - користувацьке обладнання; UPF (User Plane Function) - функція передачі даних користувачів, або функція користувацької площини; NSSF (Network Slice Selection Function) - функція вибору мережного сегменту/слайсу; NEF (Network Exposure Function) - функція забезпечення взаємодії з зовнішніми застосуваннями; NRF (NF Repository Function) - сховище мережних функцій [3].

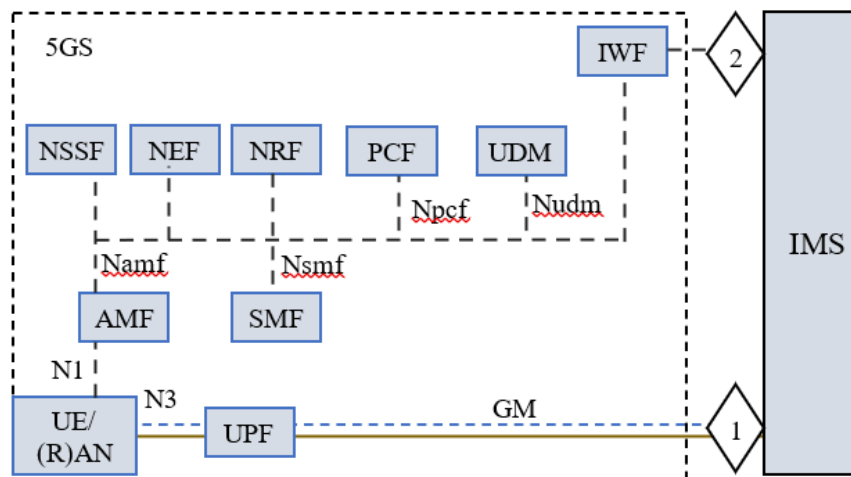


Рис. 2. Метод задіяння вузлу IWF.

ПРОЦЕДУРИ АУТЕНТИФІКАЦІЇ ТЕРМІНАЛІВ ТА ПРОМІЖНИХ МОДУЛІВ НА БАЗІ РОЮ БПЛА ЯК ЧАСТИНИ МЕРЕЖІ РАДІОДОСТУПУ 5G

Кравчук С.О., Кравчук І.М.

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. І. Сікорського, Україна*

E-mail: sakravchuk@ukr.net

PROCEDURES FOR AUTHENTICATION OF TERMINALS AND INTERMEDIATE MODULES BASED ON A SWARM OF UAVS AS PART OF A 5G RADIO ACCESS NETWORK

Authentication is a fundamental property that allows a UAV network to establish secure communication between its core components. This allows for the authentication and identification of UAVs. The purpose of this work is to carry out an analytical review of the possibilities of creating authentication procedures for a swarm of UAVs/drones, taking into account the peculiarities of swarm formation and the requirements for 5G NR.

Широке використання безпілотних літаючих апаратів (БПЛА) для різноманітних цивільних і комерційних застосувань, а також повсюдне безпроводове підключення мереж 5G і 6G можуть вимагати передових заходів безпеки для запобігання несанкціонованому доступу до конфіденційних даних [1-4]. Так само, встановлюючи заходи безпеки для мереж БПЛА, слід враховувати такі характеристики, як висока масштабованість, різноманітність пристроїв і висока мобільність.

Автентифікація (Authentication): автентифікація є фундаментальною властивістю, яка дозволяє мережі БПЛА встановлювати безпечний зв'язок між її основними компонентами. Це дозволяє автентифікувати та ідентифікувати БПЛА, які беруть участь у польоті. Надійність кожного БПЛА перевіряється за допомогою цифрового підпису і лише автентифіковані БПЛА можуть брати участь у польоті. Автентифікація також захищає мережу БПЛА від зловмисників, які видають себе за законні БПЛА.

Аутентифікація БПЛА може додатково захистити канал зв'язку, запобігаючи уособленню та повторним атакам. Розробка схем контролю доступу БПЛА, таких як механізми авторизації та автентифікації, залишається складною проблемою для дослідження в мережах БПЛА. Дійсно, будь-які неавтентифіковані БПЛА не повинні брати участь у польотних місіях для збору даних з інших БПЛА в мережі.

Протокол автентифікації об'єкта — це процес у режимі реального часу, який забезпечує впевненість у тому, що об'єкт, який аутентифікується, працює в той момент, коли цей об'єкт виконав певну дію з початку виконання протоколу.

Відоме рішення для аутентифікації одного БПЛА/дрона з використанням нової 5G радіомережі (NR) вимагає виконання двох кроків. Перший етап

охоплює аутентифікацію між дроном і базовою мережею 5G, а другий етап - аутентифікацію між дроном і станцією управління дроном. Неможливо аутентифікувати кожен дрон у рої за допомогою поточного рішення без затримки. Ключі аутентифікації між базовою станцією (BS) та користувальницьким обладнанням (UE) мають бути передані нової BS під час виконання передачі обслуговування. Зграї дронів дуже мобільні і вимагають кількох перемикачів із BS на нову BS.

Важливо також торкнутися тут деяких конкретних аспектів, які тісно пов'язані з моделлю співпраці роїв і впливають на алгоритми, що лежать в основі місії. На додаток до звичайних проблем із шифруванням та автентифікацією (всередині рою та для зв'язку між рою та GCS), ми стикаємося з двома основними додатковими проблемами.

Рій за своєю природою має динамічну структуру, і це піднімає проблему ненадійних кордонів. Рій - це система, що розвивається: БПЛА можуть приєднатися та залишити будь-коли, або з запланованих причин, або через настання несподіваної події. БПЛА може приєднатися до зграї замість того, хто покидає, або додати деяку додаткову потужність до загальної системи. Таким чином, має бути механізм для запобігання вторгненню шкідливого БПЛА. На жаль, оскільки зграї повинні підтримувати стійкість і оскільки вони динамічні, у зграї немає стабільного БПЛА.

Тому метою даної роботи є проведення аналітичного огляду можливостей створення процедур автентифікації для рою БПЛА/дронів з урахуванням особливостей формування рою та вимог до 5G NR.

Спільне використання ключів автентифікації для кожного БПЛА, як описано в 5G NR, не масштабується для груп БПЛА. У [5] була змодельована схема групової аутентифікації для нового БПЛА та аутентифікація БПЛА 5G NR. БПЛА у зграї утворюють три підгрупи, які мають різні обов'язки. Охоронні БПЛА/дрони (guard drones) - це дрони, в обов'язки яких входить відстеження догляду та приєднання дронів, а також аутентифікація нових учасників у зграях. Мережеві операції виконуються сітковими дронами (network drones). Основний сервіс надають сервісні дрони (service drones). Основні переваги запропонованого методу можна резюмувати так: 1) груповий ключ розподіляється між дронами в рої, щоб забезпечити безпечний канал зв'язку, і пропонується рішення поділитися груповим ключем із новими учасниками; 2) аутентифікація нового дрона, що бере участь у рої, вимагає двох кроків, якщо використовується рішення 5G NR. Першим кроком є підтвердження нового дрона базовою мережею, а наступним кроком є аутентифікація через станцію керування дронами. Пропонований метод пропонує рішення для групової аутентифікації, яке має кращі тимчасові та комунікаційні складності, ніж 5G NR.

У [6] представлена безпечна та спрощена схема аутентифікації для повітряної мережі з кількох БПЛА. Запропонований підхід заснований на фізичній, неклонуємої функції, яка надійно вбудована на згадку про вузли БПЛА. Запропонований підхід забезпечує безпечну роботу мережі БПЛА,

споживаючи при цьому менше бортових ресурсів, таких як заряд батареї, обчислювальна потужність та пам'ять.

В [7] запропоновано новий підхід для віддаленої ідентифікації роїв дронів. Для ефективного процесу ідентифікації між зграєю дронів та GCS кожен дрон Reader у регіоні збирає ідентифікаційну інформацію рою дронів та передає її до наземної станції для перевірки. Пропонований протокол ідентифікації скорочує час перевірки рою дронів за рахунок використання пакетної перевірки для одночасної перевірки множини дронів у рої дронів.

Можна використовувати протокол аутентифікації та узгодження ключів для встановлення безпечного зв'язку між дронами та ZSP (Zone Service Provider: IoT та IoD) у незахищеному середовищі. Проте одночасна аутентифікація великої групи дронів за допомогою ZSP призведе до серйозного навантаження сигналів аутентифікації, що неминуче погіршує якість обслуговування (QoS) систем IoD. Для правильного вирішення вищезгаданих проблем у [8] пропонується полегшений протокол групової аутентифікації, який називається liteGAP (Lightweight Group Authentication Protocol).

Література

1. Swarm of UAVs for Network Management in 6G: A Technical Review / M. A. Khan, N. Kumar, S. A. H. Mohsan, W. U. Khan, M. M. Nasralla, M. H. Alsharif, J. Zywiłek, I. Ullah // *IEEE Transactions on Network and Service Management*, 20(1), p. 741-761 (2023), <http://dx.doi.org/10.1109/TNSM.2022.3213370>
2. Kravchuk S., Afanasieva L. Formation of a wireless communication system based on a swarm of unmanned aerial vehicles // *Information and Telecommunication Sciences*. - 2019. - No 1. - 11-18 p. DOI: <https://doi.org/10.20535/2411-2976.12019.11-18>
3. Kaidenko M., Kravchuk S. Autonomous Unmanned Aerial Vehicles Communications on the Base of Software-Defined Radio. In: Ilchenko M., Uryvsky L., Globa L. (eds) *Advances in Information and Communication Technology and Systems. MCT 2019. Lecture Notes in Networks and Systems*, vol 152. Springer, Cham. pp. 289-302 (2019), https://doi.org/10.1007/978-3-030-58359-0_16
4. 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>
5. Authentication and Handover Challenges and Methods for Drone Swarms / Y. Aydin, G. K. Kurt, E. Ozdemir, H. Yanikomeroğlu // *IEEE Journal of Radio Frequency Identification*, Vol. 6, p. 220 – 228 (2022). <https://doi.org/10.1109/JRFID.2022.3158392>
6. A Lightweight Authentication Scheme for a Network of Unmanned Aerial Vehicles (UAVs) by Using Physical Unclonable Functions / Alkathairi, M.S., Saleem, S., Alqarni, M.A., Aseeri, A.O., Chauhdary, S.H., Zhuang, Y. A. // *Electronics* 2022, 11, 2921. <https://doi.org/10.3390/electronics11182921>
7. Efficient Remote Identification for Drone Swarms / K.-M. Seo, J. Kim, S. Lee, J.-W. Kwon, S.-H. Seo // *Computers, Materials & Continua* 2023, 76(3), 2937-2958, <http://dx.doi.org/10.32604/cmc.2023.039459>
8. liteGAP: Lightweight Group Authentication Protocol for Internet of Drones Systems / C. Pu, C. Warner, K.-K. R. Choo, S. Lim, I. Ahmed // *IEEE Transactions on Vehicular Technology* (2023) <https://doi.org/10.1109/tvt.2023.3335839>

МЕТОДИ ВІРТУАЛІЗАЦІЇ МЕРЕЖ МОБІЛЬНОГО ЗВ'ЯЗКУ 4G ТА 5G З МЕТОЮ ПІДВИЩЕННЯ ЯКОСТІ ОБСЛУГОВУВАННЯ

Сколець С.С., Кравчук С.О.

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна
E-mail: serskols@gmail.com, sakravchuk@ukr.net*

METHODS OF VIRTUALIZATION OF 4G AND 5G MOBILE NETWORKS AIMED AT IMPROVING SERVICE QUALITY

The rapid growth of wireless mobile traffic demands effective solutions for 4G/5G networks. Utilizing virtualization technologies and innovative approaches such as NFV, SDR, and SDN can improve service quality and reduce costs. It is crucial to consider QoS when deploying virtualized environments in the 4/5G network.

Мета роботи полягає у вивченні та аналізі різних методів віртуалізації мобільних мереж 4G/5G з огляду на їхній потенціал у покращенні якості обслуговування. Визначення ключових проблем та викликів, пов'язаних з віртуалізацією мережевих елементів у контексті 4G/5G мобільних мереж. Робота спрямована на опис рекомендацій та розуміння стратегій, які дозволять ефективно впровадити віртуалізовані середовища в мережі 4/5G з метою забезпечення оптимальної якості обслуговування для кінцевих користувачів.

Мобільний бездротовий трафік стрімко зріс завдяки широкому поширенню мобільних пристроїв. Від традиційного голосового зв'язку до соціальних мереж та електронної комерції, застосунки розвиваються швидко, що призводить до експоненційного збільшення кількості пристроїв та швидкості передачі даних. Проте мобільні мережі 4G не відповідають очікуванням, які були передбачені до 2020 року. Для досягнення покращень у пропускній здатності бездротових мереж, важливо шукати інноваційні та оптимізовані підходи до мережевих схем та інфраструктури.

Бездротові мережі 4G/5G мають неоднорідність через різноманітні технології доступу. Оператори мереж вимагають від постачальників обладнання рентабельних та енергоефективних рішень. Існують нові підходи, такі як віртуалізація мережевих функцій (NFV), програмно визначене радіо (SDR) і програмно визначена мережа (SDN).

NFV використовує віртуалізацію для консолідації мережевого обладнання на стандартних серверах і знижує витрати на обладнання та експлуатацію мережі. SDR дозволяє переналаштування радіо через програмне забезпечення і може бути використаний для швидкого розвитку бездротових стандартів. SDN дозволяє просте програмне керування мережевими ресурсами.

Досліджується можливість інтеграції NFV з SDR/SDN для мобільних

мереж 4G/5G з метою зниження витрат та підвищення відкритості та мультиорендування. Робота спрямована на інтелектуалізацію, економію та продуктивність мережі.

Рисунок 1 ілюструє гібридну архітектуру NFV, SDR і SDN. Завдяки технології NFV оператори можуть створювати наскрізну мережеву інфраструктуру за допомогою стандартної технології ІТ-віртуалізації. Цього можна досягти, реалізуючи мережеві функції за допомогою програмного забезпечення. Простіше представити або протестувати нову мережеву функцію, встановивши або оновивши пакет програмного забезпечення, що виконується серверами. Програмно визначене радіо, яке також називається програмним радіо (SR), стосується бездротового зв'язку, де модуляція передавача генерується або визначається комп'ютером. Приймач може використовувати комп'ютер для інтелектуального відновлення сигналу. SDR усуває недоліки апаратного забезпечення та допомагає розділити функції керування та функції обслуговування. Пристрої SDR забезпечують підтримку пристроїв і функцій для архітектури NFV, тоді як NFV забезпечує підтримку інфраструктури для SDN.

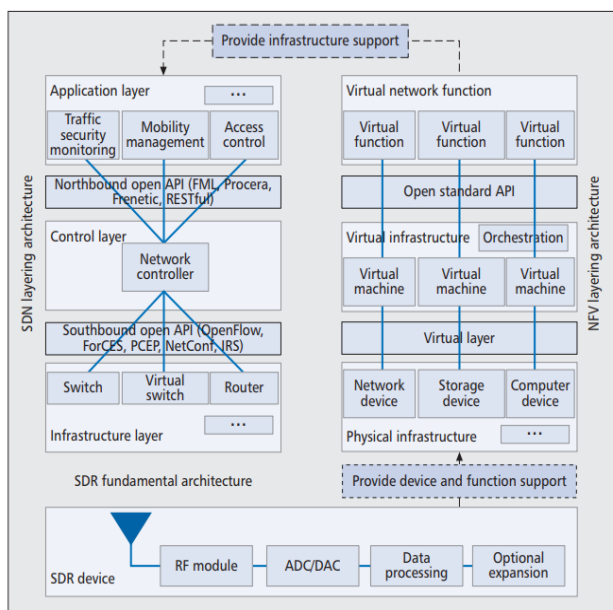


Рис.1. Архітектура NFV, SDR та SDN.

Архітектурна структура NFV зосереджена на функціональних можливостях, необхідних для віртуалізації та подальшої роботи мережі оператора.

SDR — це система радіозв'язку, у якій компоненти, зазвичай реалізовані в апаратному забезпеченні, замість цього реалізуються програмним забезпеченням на персональному комп'ютері або вбудованій системі. Технологія SDR забезпечує гнучкість і економічну ефективність, необхідні для просування комунікацій. Функції бездротового зв'язку досягаються шляхом завантаження програмного забезпечення, що пропонує різноманітні послуги радіозв'язку.

SDN: мережевий контроль у SDN відокремлений від пересилання та

NFV використовує стандартну ІТ-технологію віртуалізації для об'єднання різних типів мережевого обладнання на стандартних серверах, комутаторах і пристроях зберігання даних, що розташовані у центрах обробки даних, мережевих вузлах та в приміщеннях кінцевих користувачів. Він дозволяє розгортати та управляти мережевими та інфраструктурними послугами за допомогою програмного пакету, який працює у віртуальних машинах. NFV може бути швидко налаштованим та виведеним з експлуатації з мінімальними зусиллями.

безпосередньо програмований, що дає змогу абстрагувати базову інфраструктуру для додатків і мережевих служб і розглядати мережу як логічну або віртуальну сутність. Архітектура SDN показана в лівій частині рис. 1. Мережевий інтелект централізовано в програмних контролерах SDN. Завдяки SDN підприємства та оператори отримують незалежний від постачальника контроль над усією мережею з єдиної логічної точки, оскільки їм більше не потрібно розуміти й обробляти тисячі стандартів протоколів, а лише приймати інструкції від контролерів SDN.

Забезпечення високої якості обслуговування в мобільних мережах 4G та 5G вимагає комплексного підходу до керування різноманітними параметрами, що впливають на ефективність мережі. Одним з ключових параметрів забезпечення QoS є:

а) Швидкість передачі даних (Bitrate): Визначає граничну мінімальну ширину каналу для передачі даних і залежить від пропускної здатності мережі. Пропускна здатність, в свою чергу, визначається як кількість інформації, яку система може передавати або обробляти протягом певного часу.

б) Затримка (Delay): Затримка в процесі відправлення та прийому пакетів даних є критичним фактором для забезпечення високої якості послуг, особливо в реальному часі. Затримка вказується в мілісекундах і повинна бути мінімальною для забезпечення ефективної комунікації.

в) Втрати пакетів (Packet loss): Число втрачених пакетів вказує на ефективність передачі даних у мережі. Мінімізація втрат пакетів є важливим аспектом забезпечення надійності та стабільності мережі.

г) Рівень бітових помилок: Помилки в передачі даних, вимірювані у відношенні до кількості переданих бітів (BER), впливають на якість обслуговування і продуктивність мережі.

д) Джиттер: Зміна затримки або затримка отримання пакетів, відома як джиттер, може впливати на якість послуг, особливо для трафіку реального часу. Мінімізація джиттеру важлива для забезпечення стабільної та надійної передачі даних у мережі.

Література

1. "Software-Defined Networking: A Perspective from Within a Service Provider Environment," Бер. 2014.
2. L. R. Battula, "Network Security Function Virtualization (NSFV) Towards Cloud Computing with NFV Over Openflow Infrastructure: Challenges and Novel Approaches" IEEE ICACCI, Вер. 2014, 1622–28 с.
3. M. Sadiku and C. Akujuobi, "Software-Defined Radio: A Brief Overview," IEEE Potentials, vol. 23, no. 4, Жов./Лис. 2004, 14–15 с.
4. N. Akkari, N. Dimitriou, "Mobility Management Solutions for 5G Networks: Architecture and Services," Computer Networks, 2020.
5. S. Sun, Y. Ju, and Y. Yamao, "Overlay Cognitive Radio OFDM System for 4G Cellular Networks," IEEE Wireless Commun., 2013.

Секція 4. Інформаційні технології в телекомунікаціях

УДК 621.3:519.2

АНАЛІЗ РАДІОЧАСТОТНОГО СПЕКТРА ІЗ ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Бугайов М. В.

*Житомирський військовий інститут імені С. П. Корольова, Україна
E-mail: karunen@ukr.net*

SPECTRUM SENSING WITH INFORMATION TECHNOLOGY

Information model for signals selection in panoramic radio monitoring systems by their external parameters was developed. The essence of proposed model is to detect occupied bands of radio frequency spectrum, estimate center frequency and bandwidth of each channel, noise level and signal-to-noise ratio. Frequency channels creation allows for signal filtering and estimation of pulse durations, as well as occupancy of each channel.

На сьогоднішній день спостерігається ускладнення радіоелектронної обстановки у зв'язку зі стрімким зростанням кількості радіоелектронних засобів [1]. Найважливішу частину сучасного радіомоніторингу складає панорамний огляд широкої смуги частот і селекція сигналів [2]. Розширення ширини миттєвої смуги частот аналізу у сучасних радіоприймальних пристроях дозволяє аналізувати ділянки радіочастотного спектра (РЧС), в яких одночасно може знаходитися значна кількість аналогових та цифрових сигналів. Утворення приймальних каналів дозволить працювати в меншій смузі частот, що приведе до підвищення відношення сигнал-шум (ВСШ) і покращення показників якості оброблення. Багатоканальне оброблення сигналів у панорамних системах радіомоніторингу потребує значних обчислювальних потужностей. Тому попередня селекція сигналів за зовнішніми параметрами дозволить системі радіомоніторингу автоматично адаптуватися до подальшого оброблення, зокрема щодо вибору алгоритму розпізнавання виду модуляції.

Основне завдання попереднього (швидкого) аналізу виділеної смуги РЧС полягає у виявленні та селекції сигналів радіоелектронних засобів (РЕЗ), які в ній працюють. Для цього необхідно вирішити такі завдання:

- виявити частотні канали;
- оцінити ВСШ в каналах;
- визначити частотно-часову структуру сигналів у каналах;
- провести селекцію сигналів у каналах за їх зовнішніми параметрами.

Вирішення даних завдань дасть змогу виділити з усього потоку сигналів ті, що представляють інтерес, і провести їх детальний аналіз для визначення внутрішніх параметрів із подальшою ідентифікацією РЕЗ.

Сутність запропонованого підходу до селекції сигналів полягає у виявленні зайнятих ділянок РЧС (частотних каналів), визначенні центральної частоти та ширини смуги кожного каналу, оцінюванні рівня шуму та ВСШ.

Утворення частотних каналів дозволяє проводити фільтрацію сигналів та оцінювати тривалості імпульсів, а також завантаженість кожного каналу. Оброблення сигналу здійснюється у часових вікнах, причому через вплив випадкових факторів виміряні значення параметрів для кожного часового фрагменту будуть відрізнятися один від одного. Тому виміряні значення параметрів для кожного фрагменту сигналу записуються в асоціативні масиви, що в подальшому полегшує селекцію сигналів. Доступ до даних можна здійснювати як за номером частотного каналу (рядки таблиці), так і за параметрами сигналів (ключами), які є заголовками стовпців таблиці. Асоціативні зв'язки між даними забезпечать гнучку фільтрацію сигналів за будь-якими комбінаціями параметрів.

Розроблений алгоритм аналізу РЧС потребує великої кількості вхідних параметрів для своєї роботи. У зв'язку з цим виникає можливість гнучкого налаштування алгоритму на роботу з різними видами сигналів без зміни його структури, а лише шляхом налаштування значень деяких параметрів.

Переважну більшість параметрів можна встановити заздалегідь і не коригувати їх під час виконання алгоритму. Дані параметри є суто технічними і при їх правильному підборі вони несуттєво впливають на роботу алгоритму. Часові, частотні та амплітудні параметри можна використовувати для пошуку сигналів конкретних РЕЗ.

На рис. 1а наведено спектрограму запису сигналу у смузі частот шириною 20 МГц і тривалістю близько 3,5 с. Із даного рисунку видно, що деякі сигнали є імпульсними, а інші виглядають безперервними. На рис. 1б показано згладжений спектр потужності у смузі частот аналізу, рівень шуму та поріг, а також виділені частотні канали.

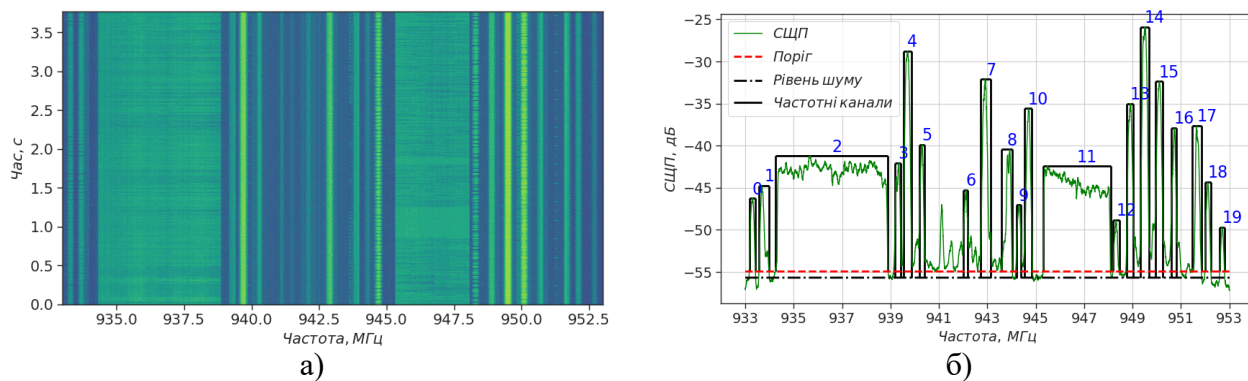


Рис. 1. Спектрограма (а) та спектр із виділеними частотними каналами (б).

Подальше каналоутворення та аналіз сигналів у часовій області у кожному частотному каналі дозволяє оцінити часову структуру сигналів та доцільність їх подальшого оброблення із урахуванням оцінок ВСШ.

Для каналів із більшим середньоквадратичним відхиленням (СКВ) значення ВСШ спостерігаються більші СКВ оцінок частотних параметрів. ВСШ у каналі на коротких інтервалах часу змінюється, в основному, через зміну потужності сигналу, що може свідчити про амплітудну модуляцію або наявність глибоких завмирань у каналі поширення.

Для апробації розробленого підходу було використано контейнер для

даних DataFrame Multi Index пакету Pandas мови програмування Python. Дана структура забезпечує багаторівневу індексацію, гнучкий доступ до даних та широкий набір інструментів для їх оброблення та модифікації, включаючи додавання записів (стовпців) з новими ключами, що утворені в результаті оброблення наявних даних [3].

На рис. 2а наведено таблицю Pandas DataFrame із оцінками значень параметрів сигналів, а на рис. 2б дану таблицю після фільтрації за шириною смуги каналу Δf відповідно до такої умови: $250 \text{ кГц} < \Delta f < 500 \text{ кГц}$. Як бачимо з даної таблиці, асоціативні зв'язки між номером каналу та рештою параметрів зберігаються. Аналогічно можна реалізувати фільтрацію рядків таблиці за будь-якими параметрами, що містяться в заголовках стовпців.

channel_new	f_0, MHz	BW, kHz	T, ms	occup, %	SNR, dB	channel_new	f_0, MHz	BW, kHz	T, ms	occup, %	SNR, dB
0	933.292	247.4	0.55	26.0	5.7	1	933.776	426.3	0.56	47.0	5.8
1	933.776	426.3	0.56	47.0	5.8	4	939.693	335.2	0.52	100.0	22.8
2	936.586	4657.2	0.00	100.0	13.0	6	941.153	376.4	0.31	30.0	2.5
3	939.296	239.4	0.55	94.0	10.7	10	943.819	410.4	0.56	95.0	10.5
4	939.693	335.2	0.52	100.0	22.8	11	944.489	271.9	0.56	24.0	10.5
5	940.280	219.0	0.24	89.0	12.4	13	948.307	326.2	0.56	10.0	6.7
6	941.153	376.4	0.31	30.0	2.5	14	948.896	263.0	0.55	97.0	17.1
7	942.150	615.0	0.55	85.0	4.7	15	949.493	341.0	0.56	98.0	25.7
8	942.571	1671.2	0.00	100.0	12.4	16	950.080	319.1	0.57	28.0	18.8
9	942.926	526.8	0.56	98.0	17.2	19	951.667	313.6	0.29	90.0	13.4
10	943.819	410.4	0.56	95.0	10.5	20	952.106	267.5	0.56	66.0	9.0
11	944.489	271.9	0.56	24.0	10.5						
12	946.707	2832.0	0.00	100.0	11.7						
13	948.307	326.2	0.56	10.0	6.7						
14	948.896	263.0	0.55	97.0	17.1						
15	949.493	341.0	0.56	98.0	25.7						
16	950.080	319.1	0.57	28.0	18.8						
17	950.699	218.9	0.55	96.0	14.0						
18	951.287	208.4	0.54	0.0	0.6						
19	951.667	313.6	0.29	90.0	13.4						
20	952.106	267.5	0.56	66.0	9.0						
21	952.695	213.3	0.17	9.0	2.2						

а) б)
Рис. 2. Таблиця з оцінками значень параметрів до (а) та після фільтрації за шириною смуги каналу (б).

В таблицю (рис. 2а) можна також додавати стовпці зі значеннями інших параметрів та змінювати існуючі. Наприклад, можна додати стовпець, в якому для заданих параметрів сигналу (кожного рядка) записувати ідентифікатор конкретного РЕЗ (стандарту радіопередачі). В подальшому цю інформацію можна використовувати для ідентифікації РЕЗ.

Використання сучасних інформаційних технологій для селекції сигналів відкриває нові можливості для всебічного та вичерпного аналізу даних, отриманих в результаті аналізу РЧС. Наукова новизна запропонованого підходу полягає у формуванні та обробленні асоціативних масивів із оцінок значень зовнішніх параметрів сигналів. Такий підхід забезпечить гнучку селекцію сигналів у панорамних системах радіомоніторингу. Розроблений алгоритм може бути використаний в існуючих та перспективних системах радіомоніторингу для ідентифікації РЕЗ та формування баз даних.

Література

1. Elmasry F. G. Dynamic Spectrum Access Decisions. Local, Distributed, Centralized, and Hybrid Designs. JohnWiley & Sons Ltd., 2021. 728 p.
2. Handbook spectrum monitoring. ITU Radiocommunication Bureau 2011. 678 p.
3. VanderPlas J. Python Data Science Handbook. Essential Tools for Working with Data. O'Reilly Media, 2017. 647 p.

МОДИФІКОВАНИЙ МЕТОД ГЕРЦЕЛЯ - БЛЕЙХУТА ВИЗНАЧЕННЯ ТОНАЛЬНИХ СИГНАЛІВ ПРИ МОНІТОРИНГУ БЕЗПРОВОДОВИХ СИСТЕМ МОБІЛЬНОГО РАДІОЗВ'ЯЗКУ

Ільницький А.І., Захарчук Л.В., Цуканов О.Ф.

Навчально-науковий інститут телекомунікаційних систем

КПІ ім. Ігоря Сікорського, Україна

E-mail: lzakharchyk-its@lll.kpi.ua

MODIFIED GOERTZEL-BLAHUT METHOD OF DETERMINING TONE SIGNALS DURING MONITORING OF WIRELESS MOBILE RADIO COMMUNICATION SYSTEMS

The determination of the spectral components of signals is carried out using the Goertzel-Blahut method without using complex values, and to determine the tone frequency, only one real coefficient is calculated for one spectral component of the signal, as well as before performing a discrete Fourier transform with a fixed sample of input signal values.

На сьогодні технічні засоби радіоперехоплення, моніторингу й радіопеленгації в мережах безпроводових систем мобільного радіозв'язку (МРЗ) реалізуються у вигляді програмно-апаратних комплексів (ПАК) різних модифікацій, які працюють в умовах часткової або повної невизначеності параметрів вхідних сигналів в реальному масштабі часу на тлі величезної кількості та різноманітності джерел радіовипромінювання (ДРВп) з найсучаснішими протоколами передачі даних. Тому найважливішими показниками ефективності ПАК при моніторингу безпроводових систем МРЗ слід вважати швидкодію, точність визначення та імовірність розпізнавання ДРВп рухомого радіозв'язку з їх інформаційним наповненням. Однак ці питання і дотепер залишаються проблематичними, що потребує подальшого розвитку ефективних методів та способів пошуку і виявлення тональних, мовних і спеціальних сигналів МРЗ у частотно-часових телекомунікаційних каналах та їх інформаційну обробку [1, 2].

Авторами доповіді проведено патентний пошук методів і способів (алгоритмів) виділення окремих спектральних складових сигналів ДРВп засобів МРЗ та обрано аналоги: непараметричний метод оцінювання власних значень MUSIC (Multiple Signal Classification); параметричний метод NDFET (Normalized Direct adaptive Frequency Technique) [3, 4]; метод (алгоритм) Герцеля-Блейхута [5, 6] - параметричний метод спектрального оцінювання, який визначено за прототип для подальших досліджень. Він заснований на використанні рекурсивного фільтра 2-го порядку з нескінченною імпульсною характеристикою (НІХ) та елементів дискретного перетворення Фур'є (ДПФ). Тут (рис. 1) масив з N вихідних відліків формується з масиву з N вхідних відліків з початком обчислення тільки після повного заповнення вхідного масиву даними. Вихідні значення $E_k(n)$ обчислюються з кожним надходженням вхідних $x(n)$. Але тільки при $n = N$ результат буде еквівалентний результату ДПФ. Тобто при $n \neq N$ потреби обчислювати

значення вихідних відліків немає. Отже, цей метод функціонально еквівалентний цифровому НІХ-фільтру 2-ого порядку, за винятком того, що кінцевий результат досягається тільки після надходження всіх N відліків. Тобто обчислення в колі прямого зв'язку проводяться при надходженні N -го вхідного відліку.

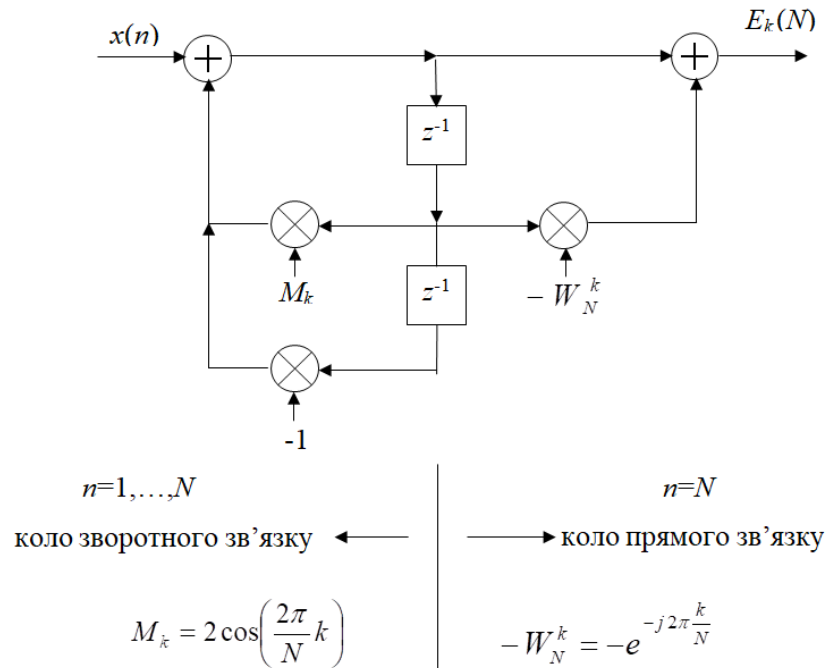


Рис. 1. Пояснення процесу розпізнавання тональних сигналів за методом Герцеля-Блейхута.

При цьому формується сумарний відлік, значення якого визначається за виразом:

$$E_k(N) = s_k(N) - W_N^k s_k(N-1), \quad (1)$$

де $W_N^k = \exp(-j2\pi k/N)$ - комплексний коефіцієнт передачі фільтра. (2)

Обчислення в колі зворотного зв'язку (рис. 1) здійснюється при надходженні кожного з n вхідних відліків ($n = 1, \dots, N$), та під час цієї фази у пам'яті зберігаються дві проміжні величини $s(n-1)$ і $s(n-2)$, які обчислюються при $s_k(0) = s_k(-1) = 0$ за такими формулами:

$$s_k(n) = M_k s_k(n-1) - s_k(n-2) + x(n), \quad (3)$$

де $M_k = 2 \cos(2\pi k/N)$ - дійсний коефіцієнт передачі фільтра. (4)

У такий спосіб на цьому етапі із кожним надходженням вхідного відліку $x(n)$ з пам'яті зчитуються значення $s(n-1)$ і $s(n-2)$, на підставі яких обчислюється нове значення $s(n)$. Після цього зі збільшенням n відбувається відновлення значень проміжних величин $s(n-1)$ і $s(n-2)$.

У існуючому методі (алгоритмі) Герцеля-Блейхута, як і в ДПФ, всі математичні дії проводяться з комплексними величинами, що в полі перетворення Фур'є ускладнює процес обчислення і суттєво погіршує його швидкодію. Для усунення цієї незручності обчислення доцільно проводити з використанням дійсних значень цих величин, тобто треба обчислювати тільки величину квадрата амплітуди спектральної складової вхідних сигналів. При цьому, в процедурі обчислення буде відсутнє визначення фази

тонального сигналу, що є не обов'язковою умовою при визначенні значення його частоти. Тобто, для визначення тональної частоти необхідно обчислювати тільки один дійсний коефіцієнт для однієї спектральної складової сигналу, а також перед виконанням N -точкового ДПФ необхідно мати буфер з N відліками значень вхідного сигналу.

Описана вище модифікація вносить зміни тільки в коло прямого зв'язку (див. рис. 1), й після простих математичних перетворень формули (1) отримуємо, що квадрат амплітуди k -ої спектральної складової сигналу обчислюється за таким простим алгебраїчним виразом:

$$E_k(N-1)^2 = s_k[N-1]^2 + s_k[N-2]^2 - M_k * s_k[N-1] * s_k[N-2], \quad (4)$$

де N – значення довжини вибірки відліків вхідного сигналу;

$s_k(n) = M_k s_k(n-1) - s_k(n-2) + x(n)$ – проміжна величина в колі зворотного зв'язку, що визначається для кожного з $n=0,1,\dots, N-1$ вхідних відліків.

Отже, для обчислення сумарного відліку спектральної складової однотонального сигналу необхідно мати тільки один дійсний коефіцієнт $M_k = 2\cos(2\pi k/N)$, а для визначення факту наявності тієї або іншої спектральної складової треба оперувати квадратом її амплітуди. Тобто використання модифікованого методу Герцеля-Блейхута вимагає наявності масиву на два значення, де N разів накопичуються проміжні величини при надходженні N вхідних відліків. Після накопичення обчислюється квадрат амплітуди спектральної складової сигналу, проміжний масив обнулюється й процес повторюється. При цьому частота появи вихідних відліків – один на N вхідних.

В презентації доповіді наведені результати імітаційного моделювання, що свідчать про працездатність та ефективність модифікаційного методу визначення тональних сигналів при моніторингу безпроводових систем МРЗ.

Література

1. Ільченко М.Ю., Кравчук С.О. Телекомунікаційні системи.–Київ: Наукова думка, 2017 730 с.
2. Ільницький А.І., Захарчук Л.В. Проблемні питання радіомоніторингу джерел і об'єктів телекомунікаційних мереж і систем та загальнонауковий концептуальний підхід до їх розв'язання / III Міжнародна науково-технічна конференція «Системи і технології зв'язку, інформації та кібербезпеки: актуальні питання і тенденції розвитку» 30 листопаду 2023 р. Військовий інститут телекомунікацій та інформації імені Героїв Крут. Збірник тез доповідей Міжнародної науково-технічної конференції.- Київ, 2023 – С.167 (ISBN 978-617-7689-05-7).
3. G. Arslan, B. Evans, F.A Sakarya and J. Pino, “Performance evaluation and real-time implementation of subspace, adaptive and DFT algorithms for multi-tone detection”, in Proc. IEEE Int. Conf. Telecommunications, (Istanbul, Turkey), pp. 884–887, Apr. 1996.
4. S.Bagchi, S.K.Mitra, An efficient algorithm for DTMF decoding using the subband NDFT, Proc. of IEEE Symposium on Circuits and Systems, Seattle, WA, USA, 28 April-3 May, 1995, vol. 3, pp.1936–1939.
5. Gerald Goertzel. An Algorithm for the Evaluation of Finite Trigonometric Series. The American Mathematical Monthly. Vol.65, №1, pp 34 – 35.
6. Blahut R.E. Fast Algorithms for Signal Processing. Cambridge. UK: Cambridge University Press, 2010, 453 p.

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ТЕЛЕКОМУНІКАЦІЯХ

Глоба Л.С., Цуканов О.Ф.

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, м. Київ, Україна*

E-mail: cukanov-o@ukr.net

APPLICATION OF ARTIFICIAL INTELLIGENCE IN TELECOMMUNICATIONS

The task of using generative artificial intelligence systems in telecommunications is considered. It is shown that the use of such systems in telecommunications will significantly increase their efficiency. Such systems make it possible to create new content by processing large volumes of deep learning neural network data. That allows you to create new applications faster and more cost-effectively.

Розглянута задача використання систем генеративного штучного інтелекту в телекомунікаціях. Показано, що використання таких систем в телекомунікаціях дозволить значно підвищити їх ефективність. Такі системи дозволяють створювати новий контент на шляхом обробки великих обсягів даних нейронних мереж глибокого навчання. Що дозволяє створювати нові додатки швидше за часом та з більшої економічною ефективністю.

У ТМ Forum [1] активно обговорюються питання, пов'язані з інтелектуалізацією як інфраструктури надання телекомунікаційних послуг, так і алгоритмів реалізації самих послуг, а також особливостей функціонування бізнесу.

На сьогодні, технологія генеративного штучного інтелекту GenAI в телекомунікаціях пройшла шлях від інструменту для створення контенту на її основі до стратегічної платформи, що використовується практично всіма постачальниками комунікаційних послуг (CSP) по всьому світу.

Генеративна система штучного інтелекту (GenAI) - це будь-яка модель машинного навчання, здатна динамічно створювати нові результати на основі нових наборів вхідних даних після навчання. Алгоритми такої моделі створюють новий контент на основі шаблонів, отриманих з наявних даних, який дає змогу знайти закономірності та визначити найкращу можливу відповідь на запитання або ситуацію, які потім генерує як вихідний результат. GenAI, отримуючи величезні обсяги даних, здатний виробити розуміння кореляцій і закономірностей всередині даних.

На відміну від традиційних підходів до машинного навчання GenAI передбачає використання фундаментальних моделей - нейронних мереж глибокого навчання, мереж, які як відправну точку для розроблення моделей використовують великі набори даних, що дають змогу створювати нові застосунки швидше й одночасно робити їх економічно ефективними.

Використання штучного інтелекту в галузі телекомунікацій формує сучасні тенденції розвитку технологій 5G [2]. Так, наприклад, Chad (Channel Access Delay) - це параметр, який використовується в стільникових телекомунікаціях для визначення затримки доступу до радіоканалу. За

допомогою технологій GenAI можна змінювати параметр Chad у телекомунікаціях, тим самим керувати доступом між кількома абонентами до загального радіоресурсу і каналів передачі даних, тим самим забезпечувати більш ефективно його використання.

У стільникових мережах, таких як GSM (Global System for Mobile Communications) та інших, Chad використовується для визначення часового вікна для передачі даних від абонента на базову станцію. Це дає змогу керувати колізіями та конкуренцією між різними абонентами під час доступу до каналу.

У загальному випадку, чим менше значення Chad, тим швидше абонент може отримати доступ до радіоканалу. Однак занадто маленьке значення Chad може призвести до перевантаження каналу і виникнення пакетних втрат даних.

У мережах GSM, CDMA та інших мобільних стандартах він використовується для координації доступу абонентів до радіоканалу. Chad допомагає знизити ймовірність колізій і оптимізувати використання доступного радіо ресурсу.

Завдяки цьому абоненти можуть передавати свої дані більш ефективно і без зайвих затримок. Ще однією сферою застосування Chad є бездротова локальна мережа (Wi-Fi). У Wi-Fi мережах Chad використовується для управління доступом між різними пристроями, підключеними до однієї точки доступу. Він допомагає регулювати час, протягом якого кожен пристрій може передавати дані, щоб уникнути конфліктів і забезпечити справедливий доступ до мережі.

Крім того, Chad може бути використаний в інших типах телекомунікаційних мереж, як-от цифрове телебачення, голосовий зв'язок через Інтернет (VoIP) та інші. У кожному разі його застосування пов'язане з необхідністю управління доступом до каналу передачі даних і оптимізації використання ресурсів.

Використання GenAI дає змогу в різних мережах і протоколах налаштувати параметри Chad механізму правильно. Неправильне налаштування може призвести до неефективного використання радіоресурсу, затримок у передачі даних і незадовільної якості зв'язку.

Його правильне налаштування і використання здатні підвищити продуктивність мережі і задовольнити вимоги користувачів в передачі даних і обміні інформацією.

Економія коштів під час використання GenAI у випадках, коли йдеться про заміну наявних функцій, може бути значною, але вона також може генерувати інші переваги - наприклад, надання операторам можливості обслуговування клієнтів, які наразі не застосовують CSP, Content Security Policy (CSP, політика захисту контенту) з міркувань вартості.

Захист контенту користувача пов'язаний із необхідністю опрацювання великих ланцюжків даних, що вимагає точності та достовірності великих мовних моделей даних (LLM - large language model).

Для того щоб GenAI міг приносити користь, йому необхідний набір знань

для навчання і функціонування. У телекомунікаційних компаніях накопичені великі набори різноманітних знань, які існують як усередині організації оператора, так і за її межами. Крім того, хмарні технології зробили революцію в телекомунікаціях.

По-перше, перехід від апаратних мережевих пристроїв до програмних додатків у хмарній інфраструктурі забезпечує простоту експлуатації та зниження вартості експлуатації.

Друге, оператори можуть монетизувати активи і запустити нові бізнес-можливості завдяки інтеграції хмари на кордоні мережі для корпоративних додатків і створення приватних мереж для промислових підприємств.

По-третє, хмара надає обчислення, зберігання даних і послуги для перетворення телекомунікаційних даних, що формуються на фізичному рівні, у зручну для людини форму.

Технології GenAI, накладені на добре керовану і сучасну платформу даних, можуть допомогти операторам у розробці нових послуг, вдосконаленні операцій і підвищити якість обслуговування клієнтів.

Оператори споживатимуть GenAI через додатки для підвищення продуктивності та якості корпоративного програмного забезпечення, але отримання найбільшої потенційної цінності очікується від обробки приватних телекомунікаційних даних засобами GenAI.

Генеративний GenAI вирішує проблеми, пов'язані з безпекою, конфіденційністю та етикою. Телекомунікаційні оператори об'єднуються, формують загальну інфраструктуру надання послуг, і вибір надійного хмарного партнера, який забезпечуватиме комплексну безпеку фізичної інфраструктури, обладнання, програмного забезпечення, і процесів набуває важливого значення. Ухвалення рішення в такому випадку не є тривіальним завданням і не може бути виконано без систем GenAI.

Оператори повинні встановлювати системні гарантії, шифрувати дані, обмежувати доступ до моделей. Щоб запобігти порушенню конфіденційності, оператори впроваджують суворий контроль даних і клієнтів, для навчання або тонкого налаштування все активніше використовують GenAI.

Вони також контролюють вихідні дані, у такий спосіб запобігаючи витоку конфіденційної інформації та впроваджуючи інструменти для забезпечення точності, справедливості, зменшення упередженості, підтримують прозорість шляхом документування своєї методології, збирають дані для навчання та забезпечення пояснюваності.

Оператори можуть використовувати аналітику для того, щоб зробити дані своїм життєво важливим джерелом інформації, але для повного використання цього потенціалу їм потрібно запровадити правильні системи, процеси та культуру.

Література

1. Mark Newman, Chief Analyst Gnerative AI, TM forum December 2023.
2. <https://inform.tmforum.org/features-and-opinion/a-week-in-telecoms-att-seeks-startups-south-korea-gets-new-5g-entrant/>

ONTOLOGY OF DIGITAL COMPUTER ONLINE LEARNING PLATFORM

Tovstii A.O., Shumskiy B.S., Sierhieiev V.V., Globa L.S.
*Educational and Scientific Institute of Telecommunication
Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine*
*E-mail: lgloba@its.kpi.ua, tovsty.arkadiy@lll.kpi.ua,
shumskiy.bohdan@lll.kpi.ua, vsierhieiev-its24@lll.kpi.ua*

ОНТОЛОГІЯ ЦИФРОВОГО НАВЧАЛЬНОГО ПРОСТОРУ ОНЛАЙН КОМП'ЮТЕРНОГО ПРАКТИКУМУ

В роботі розглянуто структуру сучасної системи онлайн-навчання, яка побудована на основі добре продуманої онтології навчальних ресурсів та характеризується інтелектуальною архітектурою. Запропонована онтологія має елементи всіх компонентів загальної онтології, включаючи класи, атрибути, відношення та інші компоненти, які необхідні для створення повноцінної моделі. Онтологічна модель розроблена із застосуванням сучасної теорії мульти-клауд систем баз даних, платформа має удосконалений інтерфейс користувача, який враховує досвід виконання та перевірки завдань кінцевими користувачами(студентами). Базова реалізація системи здійснювалася за допомогою інтерактивної навчальної платформи з відкритим кодом «Артемис». В статті представлено архітектуру системи “Артемис” та розглянуто її компоненти. Онтологічна модель включає набір компонентів та зв'язків між ними. Важливим компонентом є автоматизована функція оцінки виконання завдань, яка додає ефективності процесу оцінювання виконаних завдань, завдяки чому користувач може побачити свої помилки та результати виконання завдань, а також теоретичний матеріал щодо конкретного завдання.

Introduction. In the dynamic landscape of modern technology, the strategic integration of ontology and architecture takes on heightened significance, particularly in the context of our innovative database online training platform. Ontology serves as the intellectual framework, providing a cohesive understanding and representation of intricate database concepts. The article describes the ontological model and several architecture services of the online learning platform. The ontological model is developed using the modern theory of multi-cloud database systems, the platform has an improved user interface that takes into account the experience of performing and checking tasks by end users (students). The basic implementation of the system was carried out using the Artemis open source interactive training platform. The article presents the architecture of the Artemis system and considers its components. An ontological model includes a set of components and connections between them. An important component is the automated task evaluation function, which adds efficiency to the process of evaluating completed tasks, so that the user can see his mistakes and the results of the tasks, as well as theoretical material on a particular task.

Ontology of digital computer online learning platfor. Ontology is a system for organizing and representing knowledge within a specific domain. Ontologies are used to organize, structure, and understand information in a variety of fields, from artificial intelligence and natural language processing to biology and business intelligence. An ontology includes a set of concepts, classes, and relationships that define a subject area. It allows you to formalize knowledge and create structured models that facilitate the processing and exchange of information. Ontologies are

often used to develop intelligent systems that can understand and process information at a level that is understandable to humans. The main algorithm for creating an ontological model is based on the collection and structuring of meaningful information.

Information ontology - stores information about the objects (categories of objects) of the subject area that are intended to be displayed to the CIT user. Controlling ontology - stores information about the peculiarities of functioning of specialized program modules. Ontological presentation template - an ontology containing descriptions of software components that provide specialized thematic functions when used within an interactive document.

The actual ontology of the online learning platform includes such main components as: study course, person, feedback, estimation, exercise, events. (Fig. 1)



Fig. 1.

Proposed ontology was built using Protégé-2000 open-source ontology builder developed by Stanford University. An ontology contains a variety of relationships between classes, including associative, part-whole, inheritance, and class-data. Inheritance transfers attributes from a parent class to a child class, and all classes are related to instances through "class-data". Thus, the ontology which we build perfectly achieves our online-platform requirements.

Architecture. Main focus is on the 3 components, they are: Feedback Service, Exercise Management Service and Exercise Participation Service (Fig. 2). Those components make a major part of work on the platform. Feedback service is responsible for analyzing, estimating and making reports about each request the user sends to check their task in the exercise of the course. Moreover, it is connected with Exercise Participation Service that is mainly responsible for tracking user progress on the platform and analyzing all the information given

from Feedback Service. The next component is Exercise Management Service. It is called every time a student starts a new exercise because the intelligent system is optimized to save memory, so it creates the actual repository for the exercise only when it is requested from the end-user. Furthermore, Exercise Management Service is responsible for creating the actual courses and exercises inside them, so each time the administrator creates the course it automatically updates it to each of the users on the platform that was assigned to it.

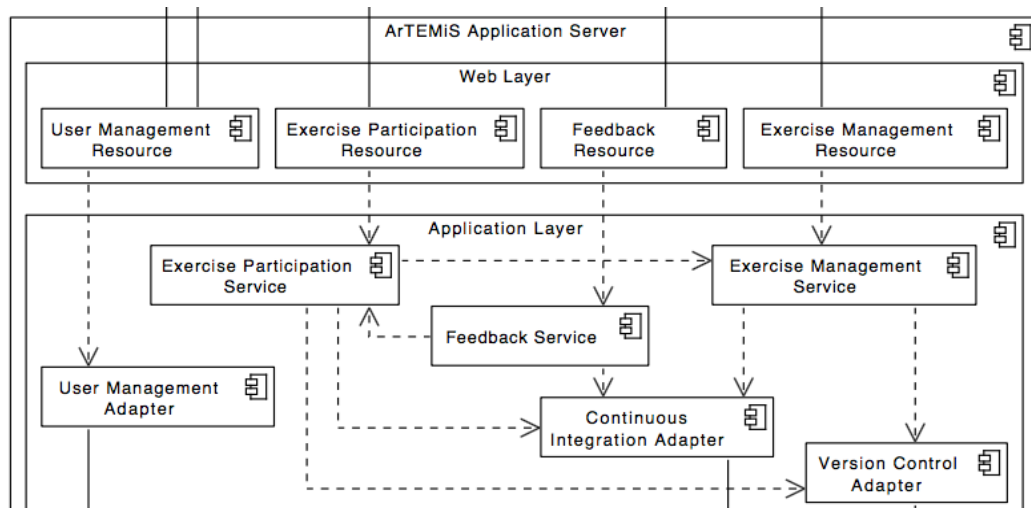


Fig. 2. Architecture of the “Artemis” open-source interactive training platform.

Conclusions. This article considers the practical experience of constructing the ontology that was built using Protégé-2000 open-source ontology builder developed by Stanford University and architecture of the digital educational space of the online computer workshop from the database course, which allows automatic verification of tasks. Using the proposed ontological model allows users to get a detailed description of errors and task results. The proposed technical solution was developed and tested together with the Technical University of Dresden for the course "Databases."

References

1. "Regulations on state certification of research (scientific and technical) institutions" [<https://zakon.rada.gov.ua/laws/show/469-98-%D0%BF/print>].
2. “Artemis”: Interactive Learning with Individual Feedback [<https://github.com/ls1intum/Artemis>]
3. Ontology Development 101: A Guide to Creating Your First Ontology [https://protege.stanford.edu/publications/ontology_development/ontology101.pdf].
4. The use of ontologies for effective knowledge modelling and information retrieval [<https://www.sciencedirect.com/science/article/pii/S2210832717300649>].
5. L. Globa, R. Novogrudska, B. Zadoienko and O.Ye. Stryzhak 2020 Ontological Model for Scientific Institutions Information Representation: [<https://ieeexplore.ieee.org/document/9467984>].
6. Ontology-Based Metamodeling [https://link.springer.com/chapter/10.1007/978-3-319-74322-6_12].

ПІДВИЩЕННЯ БЕЗПЕКИ СПОЛУЧЕННЯ ІОТ ПРИСТРОЇВ ШЛЯХОМ АНАЛІЗУ БЕЗПРОВІДНИХ СИГНАЛІВ

Педан С.І., Мельник М.В., Алексєєв М.О.

Навчально-науковий інститут телекомунікаційних

систем КПІ ім. Ігоря Сікорського, Україна

E-mail: stas.pedan@gmail.com,

8102002melpnik2@gmail.com, alexeyev@its.kpi.ua

IMPROVING SECURITY OF IOT DEVICES PAIRING BY WIRELESS SIGNALS ANALYSIS

The work is devoted to the topical issue of increasing the security of connecting simple IoT devices and protecting this process from man-in-the-middle attacks. Simple devices are the basis of the rapid development of the IoT sphere. A rapid increase in the number of simple devices is accompanied by an increase in the number of attacks in the field of security of their connection and communication. Simple devices do not have the technical resources to implement complex cryptographic protocols, which reduces their level of security, for example, the inability to protect against man-in-the-middle attacks. The paper proposes a method of increasing the security of connection of IoT devices by determining the proximity of their location based on the results of the analysis of the characteristics of the wireless signal. Calculations are presented that prove that the proposed method ensures the security of connecting IoT devices at a close distance and protection against man-in-the-middle attacks.

Інтернет речей (Internet of Things, IoT) – це нова парадигма, в якій велика кількість пристроїв та датчиків співпрацює шляхом комунікації через Інтернет, надаючи інноваційні сервіси для різних викликів і проблем сучасного життя [1]. Застосування технологій IoT забезпечує соціальний, технологічний та фінансовий розвиток суспільства, забезпечуючи розумне управління рухом транспортних засобів, безпекою і спостереженням, автоматизацією сільського господарства, охороною здоров'я та медициною, розумними містами та будинками, енергоспоживанням [2].

Останній звіт «Стан IoT – Весна 2023» від IoT Analytics [3] показує, що кількість глобальних підключень IoT зросла на 18% у 2022 році до 14,3 мільярдів активних пристроїв IoT. Хоча прогнозувалося, що зростання у 2023 році буде дещо нижчим (на 16% або до 16 мільярдів активних пристроїв), ніж у 2022 році, очікується, що кількість підключень пристроїв IoT продовжуватиме зростати протягом багатьох наступних років. Серед технологій комунікації IoT пристроїв домінують Wi-Fi, Bluetooth та стільниковий зв'язок. Bluetooth підключення займають 27% від загальної кількості. Bluetooth Low Energy (BLE) забезпечує надійне підключення при обмеженому споживанні енергії, що є кращим варіантом IoT пристроїв з живленням від батареї. Прикладами таких пристроїв можуть бути датчики розумного дому або трекери персональних речей.

Хоча складні системи відіграють важливу роль в IoT, саме розробка, інтеграція та використання простих пристроїв насправді сприяє широкому впровадженню та впливу цієї технології [4]. Прості пристрої, такі як датчики і приводи, є основою Інтернету речей. Вони забезпечують безперебійне з'єднання та зв'язок між різними об'єктами в повсякденному житті: розумні системи безпеки

будинку використовують прості пристрої, такі як датчики руху та датчики дверей, щоб виявляти будь-яку надзвичайну активність та надсилати сповіщення власникам будинку. В основі пристроїв IoT, включаючи перелічені прості пристрої, лежить їх здатність спілкуватися та ділитися даними.

В той же час, прості пристрої IoT ставлять перед розробниками серйозні задачі по забезпеченню їх безпеки. Більшість простих пристроїв IoT за своєю суттю незахищені через їхні малі або обмежені розміри, які здатні вмістити лише малопотужні вбудовані мікроконтролери, прості датчики, виконавчі механізми, блоки живлення та інші крихітні електронні компоненти. Це обмеження розміру в поєднанні з вимогами до низького енергоспоживання, простими або базовими операційними системами та обмеженою обчислювальною потужністю часто перешкоджає застосуванню передових або навіть сучасних криптографічних методів, не кажучи вже про цілі рішення безпеки [5]. Активне розповсюдження простих IoT пристроїв у повсякденному житті у поєднанні з низькою захищеністю робить їх прибутковою мішенню для кіберзлочинців.

Для сполучення з простими IoT пристроями, які не мають інтерфейсу користувача (дисплею, мікрофону, динаміку, засобів введення інформації, таких як клавіатура) і, як наслідок, можливості ввести або підтвердити ключ доступу, використовують метод JustWorks[6]. Для BLE пристроїв він забезпечує найбільш прийнятний режим сполучення, оскільки майже всі BLE IoT пристрої не мають жодних можливостей введення та виведення інформації, наприклад лампочки, розумні замки, холодильники, брелоки, монітори серцевого ритму. Основною особливістю цього режиму сполучення є те, що для завершення процедури з'єднання не потрібна автентифікація[7]. Будь-хто може підключитися до будь-якого пристрою BLE, який використовує Just Works. В результаті, створене з'єднання захищене від пасивного прослуховування завдяки шифруванню, але безсиле перед атакою посередника (Man in the middle, MITM). Сценарій заволодіння IoT пристроєм зловмисником в результаті атаки посередника представлений на рис. 1.

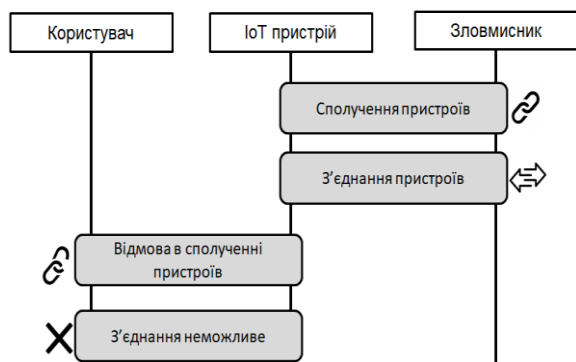


Рис. 1. Актуальний сценарій заволодіння IoT пристроєм зловмисником в результаті атаки посередника

той час як пристрій IoT продовжує надсилати пакети. Два жести, тобто переміщення смартфона до пристрою IoT і від нього, а також обертання смартфона, призводять до значної (близько 15 дБ) зміни потужності отриманого сигналу (RSS) через швидку зміну затухання та поляризації антени відповідно. По рівню кореляції RSS-варіацій з показами датчиків руху смартфона (акселерометер та гіроскоп) можливо виконати надійне виявлення близькості пристроїв. Це дозволяє

Задачею роботи є підвищення безпеки методу сполучення простих BLE IoT пристроїв для захисту від атак посередника. Дослідники з Microsoft Research запропонували метод Move2Auth[8], що забезпечує автентифікацію простих IoT пристроїв на основі визначення їх близькості. Метод вимагає від користувача тримати смартфон і виконувати один із двох жестів рукою (випадково вибраних смартфоном) перед пристроєм IoT, у

ефективно розрізняти близькі та далекі пристрої і таким чином захистити процедуру сполучення двох близьких пристроїв від далеко розташованого зломисника, який може довільно підсилити потужність передачі свого сигналу.

В даній роботі пропонується замість використання специфічних рухів смартфоном піднести його на максимально близьку відстань до IoT пристрою і провести взаємну автентифікацію по потужності безпроводного сигналу.

Потужність сигналу, яку вимірює перший пристрій, зменшується зі збільшенням відстані до другого пристрою. Таку залежність можна описати наступною формулою:

$$RSSI_{d1} = RSSI_{d0} - 20\log\left(\frac{d1}{d0}\right) \quad (1)$$

де $d0$ – початкова відстань між пристроями, $d1$ – кінцева (збільшена) відстань між пристроями, $RSSI_{d0}$ – потужність сигналу на відстані $d0$, $RSSI_{d1}$ – потужність сигналу на відстані $d1$.

Відповідно до отриманих експериментальних даних, RSSI для відстані до 10 сантиметрів має середнє значення -10dBm . Для того, щоб перевести dBm у вати, будемо використовувати наступну формулу:

$$P(W) = \frac{10^{\frac{P(\text{dBm})}{10}}}{1000}, \quad (2)$$

де $P(W)$ – потужність сигналу у ватах, $P(\text{dBm})$ – потужність сигналу у dBm . Таким чином, відповідно до формули [1], якщо зломисник знаходиться на відстані 10 метрів від IoT пристроя, рівень його сигналу буде на $20\log\left(\frac{d1}{d0}\right) = 20\log\left(\frac{10}{0.1}\right) = 20 \cdot 2 = 40\text{dBm}$ менше, ніж аутентичного пристрою на відстані 10 сантиметрів при однаковій вихідній потужності антени BLE. Для того, щоб створити на IoT пристрої ілюзію знаходження пристрою на близькій відстані, зломиснику необхідно збільшити потужність сигналу на 40 dBm , або 10 Ват за формулою [2]. Враховуючи правила FCC та ETSI, максимальна вихідна потужність антени, яка дозволена протоколом BLE, становить 20 dBm .

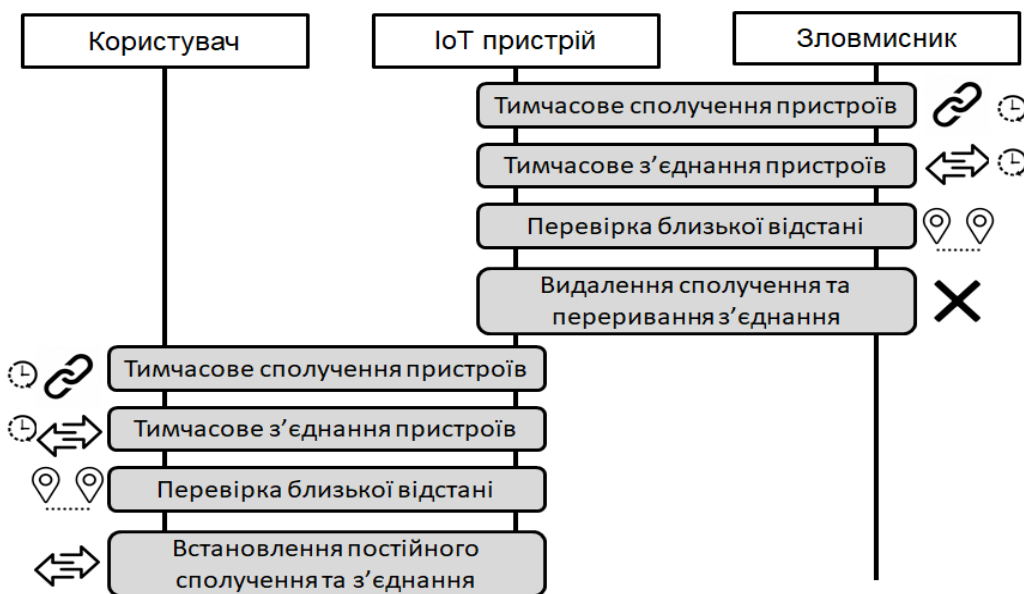


Рис. 2. Сценарій захисту від заволодіння IoT пристроєм зломисником з використанням запропонованого методу.

Таким чином, запропонований метод забезпечує захист процесу сполучення з IoT пристроєм на близькій відстані.

Висновки.

1. Активний розвиток технологій IoT та збільшення кількості пристроїв підвищує вимоги до безпеки сполучення та комунікації таких пристроїв.

2. Прості пристрої, що є основою індустрії IoT, не мають технічних ресурсів для реалізації складних криптографічних протоколів, що знижує рівень їх безпеки, наприклад, неспроможність захиститися від атак посередника.

3. Безпека сполучення простих IoT пристроїв може бути підвищена за рахунок їх автентифікації по близькості розташування шляхом аналізу потужності безпроводного сигналу (такого, як BLE).

4. Приведені розрахунки, які доказують, що запропонований метод забезпечує безпеку сполучення IoT пристроїв на близькій відстані та захист від атак посередника.

Література

1. Sachin Kumar, Prayag Tiwari and Mikhail Zymbler, Internet of Things is a revolutionary approach for future technology enhancement: a review, Journal of Big Data, 6, Article number: 111 (2019): Онлайн: <https://journalofbigdata.springeropen.com/articles/10.1186/s40537-019-0268-2>
2. S Choudhary, G Meena, Internet of Things: Protocols, Applications and Security Issues, Procedia Computer Science, Volume 215, 2022, Pages 274-288: Онлайн: <https://www.sciencedirect.com/science/article/pii/S1877050922021019>
3. IoT Analytics, State of IoT 2023: Онлайн: <https://iot-analytics.com/wp/wp-content/uploads/2023/05/Insights-Release-State-of-IoT-2023-Number-of-connected-IoT-devices-growing-16-to-16.0-billion-globally.pdf>.
4. Tomorrow Bio, Understanding IoT: How Simple Devices Can Drive Big Changes, 2023: Онлайн: <https://www.tomorrow.bio/post/understanding-iot-how-simple-devices-can-drive-big-changes-2023-06-4732281520-iot>
5. Mohammed Aziz Al Kabir, Wael Elmedany & Mhd Saeed Sharif (2023) Securing IoT Devices Against Emerging Security Threats: Challenges and Mitigation Techniques, Journal of Cyber Security Technology, 7:4, 199-223: Онлайн: <https://doi.org/10.1080/23742917.2023.2228053>.
6. AN1302: Bluetooth Low Energy Application Security Design Considerations in SDK v3.x and Higher, Silicon Laboratories: Онлайн: <https://www.silabs.com/documents/public/application-notes/an1302-bluetooth-application-security-design-considerations.pdf>.
7. Karim Lounis, Mohammad Zulkernine. Bluetooth Low Energy Makes "Just Works" Not Work. Cyber Security in Networking Conference, Oct 2019, Quito, Ecuador. fihal-02528877: Онлайн: <https://hal.science/hal-02528877/document>
8. Zhang, Jiansong, Zeyu Wang, Zhice Yang, and Qian Zhang. "Proximity based IoT device authentication." In IEEE INFOCOM 2017-IEEE conference on computer communications, pp. 1-9. IEEE, 2017: Онлайн: <https://ieeexplore.ieee.org/abstract/document/8057145>.

ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ПЕРЕДАЧІ МЕДІА ДАНИХ З ВИКОРИСТАННЯМ ЗАВАДОСТІЙКОГО КОДУВАННЯ

Педан С.І., Романович О.Д., Алексєєв М.О.
*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна*
*E-mail: stas.pedan@gmail.com,
lesharomanovich4@gmail.com, alexeyev@its.kpi.ua*

QUALITY ASSURANCE OF MEDIA DATA TRANSMISSION USING NOISELESS CODING

Робота присвячена актуальному питанню забезпечення якості передачі медіа даних в гетерогенній мережі за допомогою використання завадостійкого кодування. По результатам проведеного аналізу протоколів та алгоритмів завадостійкого кодування прикладного рівня для передачі відео даних високої якості були відібрані алгоритми Ріда-Соломона та Raptor, стандартизовані для протоколу Mpeg Media Transport для передачі 4K/8K HEVC відео, для моделювання ефективності їх роботи. Результати моделювання показали, що застосування алгоритму Ріда-Соломона можливо для невеликої швидкості відео потоку (2K та нижче), та одиничних помилок в каналі передачі. Raptor алгоритм забезпечує високу якість передачі відео 4K та 8K в умовах як одиничних, так і серійних помилок в каналі передачі, але потребує значно більших обчислювальних ресурсів.

The work is devoted to the urgent issue of ensuring the quality of media data transmission in a heterogeneous network using interference-resistant coding. Based on the results of the analysis of application-level interference-resistant coding protocols and algorithms for the transmission of high-quality video data, the Reed-Solomon and Raptor algorithms, standardized for the Mpeg Media Transport protocol for the transmission of 4K/8K HEVC video, were selected to simulate their performance. The simulation results showed that the application of the Reed-Solomon algorithm is possible for a small speed of the video stream (2K and below) and single errors in the transmission channel. The Raptor algorithm provides high-quality 4K and 8K video transmission in the conditions of both single and serial errors in the transmission channel, but requires significantly more computing resources.

Зростаючі вимоги до продуктивності програмного забезпечення призводять до необхідності забезпечення високих обчислювальних можливостей пристроїв та високої швидкості їх комунікації. Ринок мобільних пристроїв, який є одним з головних драйверів розвитку сучасних високих технологій, також рухається шляхом, що відповідає вимогам клієнтів, збільшуючи функціональні можливості пристроїв та швидкість передачі даних.

Основною проблемою, з якою стикається індустрія мобільних пристроїв, є розрив між алгоритмічною складністю, продуктивністю процесора та доступною ємністю енергії (заряд акумулятора). Закон Шеннона передбачає, що продуктивність передачі даних покращиться вдвічі за 8,5 місяців, тоді як продуктивність процесора покращиться вдвічі за 18 місяців. Крім того, виробникам акумуляторів потрібно від 5 до 10 років, щоб

досягти порівнянню збільшення щільності енергетичної ємності[1].

За останні кілька десятиліть мобільний зв'язок став свідком надзвичайного прогресу, змінивши спосіб підключення, спілкування та доступу до інформації. Розгортаємо основні технології, які забезпечують цей прогрес.

5G забезпечує вищу швидкість передачі даних, меншу затримку та покращену надійність порівняно з попередніми поколіннями, а також може підтримувати набагато більшу кількість пристроїв. Все це дозволяє виконувати швидше і ефективніше більш складні задачі в таких сферах, як віртуальна та доповнена реальність, автономні транспортні засоби, Інтернет речей (IoT) [2].

Нещодавно був прийнятий стандарт Wi-Fi 7 (802.11be), який забезпечує нові варіанти використання напрямках багатокористувацької AR/VR/XR, 3D навчання, електронних ігор, гібридної роботи, промислового IoT та автомобільної індустрії. Прогнозується, що Wi-Fi 7 у 2024 році буде впроваджений на більш ніж 233 мільйонах пристроїв, та 2,1 мільярдів пристроїв до 2028 року [3].

Відбувається розвиток мережі IoT пристроїв, що вимагають мультимедійних комунікацій високої пропускну здатності та низької затримки. Прикладом можуть бути служби моніторингу розумного міста в реальному часі, такі як системи камер спостереження, відстеження транспортних засобів, контроль руху, моніторинг навколишнього середовища, виявлення руху об'єктів тощо.

Окрім IoT, відбувається стрімкий розвиток Інтернету транспортних засобів (IoV). Мобільність терміналу, швидкість та відповідні мобільні аспекти є факторами, що впливають на якість доставки бездротового відео в рамках інтелектуальних транспортних систем (ITS) і комунікацій Vehicle-to-everything (V2X) [4].

Очікується, що в найближчий час загальний глобальний трафік мобільних даних досягне 130 ексабайтів на місяць, а в 2029 році цей показник зросте приблизно в 3 рази та досягне 403 ексабайти на місяць. Прогнозований ріст трафіку до 2029 р. передбачає припущення, що початкове впровадження послуг типу XR, включаючи AR, VR і змішану реальність (MR), відбудеться у другій частині прогнозованого періоду. За оцінками, на кінець 2023 року відеотрафік становив 73 відсотки всього трафіку мобільних даних.

Відповідно до останнього звіту компанії Ericsson про мобільність очікується, що до 2027 року об'єм передаваного відеоконтенту зросте втричі та складатиме майже 80 відсотків мобільного трафіку[5].

Продукти та технології, що використовують відео, помітно просунулися за роздільною здатністю за останні роки, перейшовши до надвисокої роздільної здатності 4K та 8K. Це стало можливим завдяки розвитку комплексу технологій як то збільшення потужності DSP і GPU, а також розвитку мережевих технологій, описаних вище. Розвитку 8K відео сприяє розробка екосистеми для створення такого контенту (професійні камери та камери мобільних телефонів) та вдосконалення ефективності кодування 8K відео (HEVC кодек).

Збільшення роздільної здатності відео контенту та нові можливості мережевих технологій потребували створення нових стандартів ефективного кодування відео та транспортних протоколів. Тому у 2013 році був прийнятий MPEG-H стандарт, частиною якого став стандарт стиснення відео H.265 (HEVC), а також протокол передачі медіа контенту на прикладному рівні MPEG Media Transport (MMT).

Гібридна доставка медіа відноситься до поєднання доставки медіа

компонентів через різні типи мережі, що є однією з найважливіших властивостей ММТ. Однак при передачі медіа даних виникає ряд проблем:

1. Неоднорідність мереж. Гетерогенні бездротові мережі відрізняються залежно від обмежень пропускну здатності, затримок та частоти втрат пакетів. Ці різні фізичні властивості спричиняють асиметричний зв'язок для передачі відео, і, отже, можуть знизити загальну якість потокового передавання.

2. Порушений порядок пакетів. Поширення даних гетерогенними шляхами з різними швидкостями та коливаннями пропускну здатності створює проблему неперевантажених пакетів.

3. Коли в буфері призначення зберігається багато пакетів, які очікують відкладених пакетів, буфер може переповнитися та заблокуватися.

4. Прострочені пакети. Пакети відеоданих, які надходять до пункту призначення після кінцевого терміну декодування відомі як прострочені пакети.

Пряма корекція помилок (FEC) допомагає знизити вплив перелічених вище факторів та покращити якість передачі медіа даних. Стандарт MPEG-H визначає декілька алгоритмів FEC прикладного рівня, які можуть використовуватися з протоколом ММТ. Прикладами таких алгоритмів є код Ріда-Соломона (RS), Raptor, LDGM.

Необхідний компроміс між пропускну здатністю/затримкою та надлишковістю FEC. Хоча більша надлишковість призводить до кращої відновлюваності, вона також збільшує об'єм даних для передачі і рівень використання об'єму каналу передачі. Отже, ймовірність перевантаження, зміни порядку пакетів, затримки декодування FEC і загальної затримки передачі даних підвищується, особливо за наявності пакетних втрат. Тому для мінімізації цих проблем і максимізації відновлюваності потрібен адаптивний FEC, для якого можна змінювати параметри (наприклад, розмір пакета і надлишковість) відповідно до стану каналу мережі або на основі важливості вмісту даних. Наприклад, сильніший FEC може використовуватися в каналі з більшими втратами, але такий рівень не потрібен у більш стабільному каналі з меншим відсотком втрат, або більш надійний FEC також може використовуватися лише для I-кадрів, а не для B- або P-кадрів відео.

В даній роботі проведено моделювання ефективності використання FEC алгоритмів з невеликою максимальною кількістю інформаційних та надлишкових символів блоку даних (RS) у 256 символів та фонтанного коду Raptor, який має мінімальне обмеження у 8192 інформаційних символів, але набагато більшу кількість надлишкових символів.

Тестова схема оцінки ефективності завадостійких алгоритмів представлена на рис. 1.

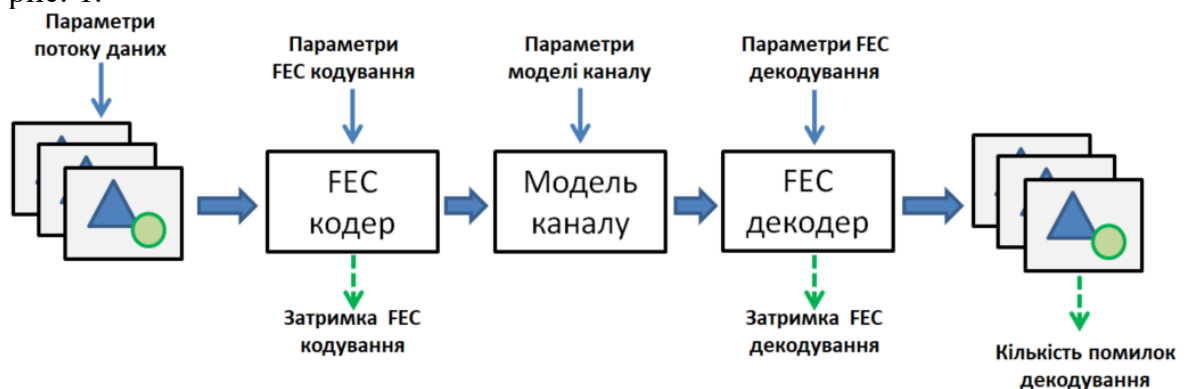


Рис. 1. Схема оцінки ефективності алгоритмів завадостійкого кодування.

Першим кроком є формування потоку зображень, який імітує потік ключових кадрів відео заданого об'єму (для 2K відео – 20 Mbps, 4K – 60 Mbps, 8K – 100 Mbps). Дані передаються на FEC кодування, для якого використовувались різні значення проміжку формування блоку (що визначало розмір блоку в залежності від швидкості потоку даних), а також різний рівень надлишковості кодування. Потік оригінальних та надлишкових даних передавався на модель каналу, яка імітувала одиничні та серійні втрати в каналі заданої якості. Остаточним кроком було FEC декодування.

В результаті проведених експериментів були отримані значення затримки кодування та декодування, а також статистика кількості помилок декодування. Аналіз результатів показав, що RS код забезпечує мінімальну затримку кодування та декодування, та має низкі показники кількості помилок декодування при одиничних втратах в каналі. Але при серійних втратах RS код має високій рівень помилок декодування по причині малого розміру блоку для заданих швидкостей відео даних. Raptor код по причині більшої кількості операцій алгоритму має більшу затримку декодування, але продемонстрував мінімальну кількість помилок декодування як для одиничних, так і серійних втрат в каналі завдяки значно більшій максимальній ємності блоку у порівнянні з RS.

Висновки. Був проведений аналіз протоколів та алгоритмів завадостійкого кодування прикладного рівня для передачі відео даних високої якості.

1. Проведено модулювання ефективності використання алгоритмів RS та Raptor для різних швидкостей потоку відео даних, а також параметрів моделі каналу передачі.

2. По результатам моделювання зроблений висновок, що застосування RS алгоритму можливо для невеликої швидкості відео потоку (2K та нижче), та одиничних втратах в каналі передачі. Raptor алгоритм забезпечує високу якість передачі відео 4K та 8K в умовах як одиничних, так і серійних втратах в каналі передачі, але потребує значно більших обчислювальних ресурсів.

Література

1. Wu, Jerry & Shen, Yin-Lin & Reinhardt, Kitt & Szu, Harold & Dong, Boqun. (2013). A Nanotechnology Enhancement to Moore's Law. Applied Computational Intelligence and Soft Computing. 2013: Онлайн: https://www.researchgate.net/publication/258393482_A_Nanotechnology_Enhancement_to_Moore's_Law
2. A Timeline from 1G to 5G: The Evolution of Mobile Communication: Онлайн: <https://www.mpirical.com/blog/the-evolution-of-mobile-communication>
3. Wi-Fi CERTIFIED 7: Онлайн: <https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-7>
4. Afzal, Samira, Vanessa Testoni, Christian Esteve Rothenberg, Prakash Kolan, and Imed Bouazizi. "A holistic survey of wireless multipath video streaming." *arXiv preprint arXiv:1906.06184* (2019): Онлайн: <https://arxiv.org/pdf/1906.06184.pdf>
5. Mobile data traffic outlook: Онлайн: <https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/mobile-traffic-forecast>

**ОГЛЯДОВИЙ АНАЛІЗ ТЕХНОЛОГІЙ
КОНТЕЙНЕРИЗАЦІЇ ДЛЯ ВИКОРИСТАННЯ У ГЕТЕРОГЕННОМУ
СЕРЕДОВИЩІ ІЗ ДИНАМІЧНОЮ АРХІТЕКТУРОЮ**

Шелест Є.В., Алексєєв М.О., Педан С.І.

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна*

E-mail: krohaenot522@gmail.com, alexeyev@its.kpi.ua, stas.pedan@gmail.com

**AN OVERVIEW ANALYSIS OF CONTAINERIZATION TECHNOLOGIES FOR USE
IN A HETEROGENEOUS ENVIRONMENT WITH A DYNAMIC ARCHITECTURE**

The work is devoted to the actual problem of effective use of computing resources of computer clusters for the execution of containerized programs. There are many containerization technologies and the execution of containerized programs in a cluster environment, but all of them are oriented to execution in computing environments with groups of the same type of working computing nodes, the number and configuration of which are mostly unchanged throughout the entire period of cluster operation. To date, there is no comprehensive analysis of the possibility of using such technologies in a heterogeneous environment with a dynamic architecture involving personal or public computing devices. In order to solve this problem, this paper proposes comparison criteria and conducts an overview analysis of existing containerization technologies using expert evaluation methods.

У той час, коли попит на інформаційні обчислювальні ресурси збільшується в зв'язку зі зростаючими обсягами даних, потребуючих обробки, актуальними стають проблеми ефективного керування такими ресурсами з можливістю змінювати їх кількість та потужність відповідно до поточного навантаження, яке може динамічно змінюватись з часом як впродовж доби так і в більш довготривалому періоді. Основним рішенням цих проблем є обчислювальні хмарні сервіси, які дозволяють варіювати кількістю обчислювальних вузлів розподілених інформаційних середовищ. Їх послуги зводяться до використання груп однотипних робочих обчислювальних вузлів, конфігурація і операційні середовища яких є однаковою в рамках групи, а кількість змінюється в залежності від навантаження. В той же час, в корпоративних мережах існує велика кількість одиниць комп'ютерної техніки, які є ввімкненими впродовж всього робочого часу і можуть розглядатись як обчислювальні вузли для побудови власної корпоративної хмари. У такої хмари є багато недоліків порівняно з комерційними хмарними рішеннями, але є дві переваги, які дозволяють позитивно оцінювати доцільність її створення, а саме відносна низька вартість володіння і можливість повної ізоляції, що дозволяє обробляти дані з обмеженим доступом. Обчислювальні вузли такої хмари мають відносно короткостроковий і недетермінований час життя своїх обчислювальних агентів, а конфігурація і операційне середовище є гетерогенним. Для побудови інформаційної обчислювальної системи в попередніх роботах [1], [2] було прийняте рішення використовувати архітектурний підхід

мікросервісів і технології контейнеризації через їх кросплатформеність. В даному випадку термін «технологія контейнеризації» включає в себе програмні компоненти, які працюють на різних рівнях абстракції, а саме:

- середовище виконання контейнерів, тобто компоненти, які створюють, запускають, та керують власне контейнерами;
- платформа контейнеризації, яка, в поєднанні із середовищем виконання та іншими компонентами, дозволяє запускати необхідні контейнеризовані мікросервіси в контейнері та дозволяти контейнерам комунікувати між собою;
- оркестратор контейнерів, який є надбудовою над платформою контейнеризації, яка дозволяє масштабувати кількість копій одного і того самого контейнера, балансувати навантаження між ними керувати життєвим циклом і так далі.

Для проведення комплексного аналізу технологій контейнеризації щодо можливості використання у гетерогенному середовищі з динамічною архітектурою із залученням обчислювальних пристроїв персональних або загального користування пропонується виділити критерії для їх оцінки, після чого за допомогою експертних методів вибрати ті технології, які найбільш їм відповідають.

Середовища виконання контейнерів. Для оцінки середовища виконання контейнерів пропонується виділити наступні критерії, а для врахування ступеню їх впливу на загальну оцінку за допомогою експертного методу попарного порівняння із залученням 5 експертів, після аналізу узгодженості оцінок було отримано наступні вагові коефіцієнти.

Табл. 1. Критерії для оцінки середовищ виконання контейнерів із ваговими коефіцієнтами.

№	Назва критерію	В.коэф.
1	Ліцензія використання середовища виконання контейнерів.	0.125
2	Операційні системи, на яких є можливість запустити додаток.	0.75
3	Складність використання інтерфейсу додатку.	0.125
4	Рівень безпеки з точки зору ізолюваності контейнерів для власника обчислювального вузла.	0.875
5	Сумісність із Kubernetes. Kubernetes є одним із найпопулярніших контейнерних оркестраторів і сумісність контейнерного виконавця із ним є важливим критерієм.	0.5
6	Сумісність зі Swarm. Використання такого засобу оркестрації як Docker Swarm є одним з найзручніших та найлегших варіантів для побудови мікросервісної архітектури.	0.93
7	Частота оновлень додатку, яка свідчить як часто виконуються оновлення та виправлення помилок.	0.125
8	Легковажність додатку, тобто скільки необхідно ресурсів для його роботи.	0.5
9	Здатність до роботи в динамічній архітектурі – виражає операційну складність створення та видалення середовища для виконання контейнера.	0.93

Результати експертного оцінювання найбільш популярних середовищ виконання контейнерів за пропонованими критеріями і ваговими коефіцієнтами наведені у таблиці 2.

Табл. 2. Порівняльна таблиця середовищ виконання контейнерів.

Критерій	Ліцензія	Опер. системи	Складн. інтерф.	Рівень безп.	Сум. із Kuber.	Сум. із Swarm	Част. оновл.	Легковажність	Дин. арх.
Ваг. коеф.	0.1	0.8	0.1	0.8	0.6	1	0.1	0.5	0.93
Технологія									
containerd	3	4	4	2.5	3	7	3.5	4	3
CRI-O	3	2	3	3	3	1	3.5	3	3
Linux containers	1	2	2	1.5	1	1	2	1.5	1
rkt	3	2	1	3	3	1	1	1.5	3

Після проведення необхідних розрахунків було проведено ранжування розглянутих контейнерних середовищ:

1. containerd (19.83)
2. CRI-O (19.3)
3. Rkt (10.84)
4. Linux containers (6.58)

За отриманими результатами можна зробити висновок, що containerd підходить до виконання поставленої задачі найбільше.

Платформи контейнеризації. Для експертної оцінки платформ контейнеризації, пропонується виділити наступні критерії і були отримані наступні вагові коефіцієнти.

Табл. 3. Критерії для оцінки платформ контейнеризації.

№	Назва критерію	В. коеф.
1	Продуктивність	0.4
2	Ресурси, якими може оперувати платформа контейнеризації.	0.2
3	Рівень безпеки.	0.8
4	Операційні системи.	0.6
5	Підтримка оркестраторів.	0.2
6	Легковажність додатку.	0.4
7	Здатність до роботи в динамічній архітектурі.	0.8

Результати експертного оцінювання найбільш розвинених платформ контейнеризації за пропонованими критеріями і ваговими коефіцієнтами наведені у таблиці 4.

Табл. 4. Порівняльна таблиця платформ контейнеризації.

Критерій	Прод-ть	Ресурси	Рівень безпеки	Операційні системи	Підтримка оркестраторів	Легковажність	Динамічна архітектура
Ваг. коеф.	0.4	0.4	0.6	0.6	0.2	0.4	0.8
Платформи							
Docker	3	4	3,33	6	4	3,5	4
LXC/LXD	4	4	3,33	2	2	4,5	4
Singularity	3	2	3,33	2	4	2	2

Ранжування платформ за кінцевими оцінками наступне:

1. Docker (13.79)
2. LXC/LXD (11.79)
3. Singularity (8.99)

За отриманими результатами можна зробити висновок, що Docker є найбільш підходящою платформою контейнеризації для виконання поставленої задачі з побудови мікросервісної архітектури з динамічною архітектурою.

Оркестратори контейнерів. Для експертної оцінки систем оркестрації запропоновані наступні критерії і отримані наступні вагові коефіцієнти.

Табл. 4. Критерії для оцінки систем оркестрації контейнерів.

№	Назва критерію	В.коэф.
1	Тип контейнерів, із якими оркестратор здатний працювати	0.4
2	Масштабованість. Тобто, кількість контейнерів, які оркестратор може одночасно запустити та керувати	0.07
3	Наявність автоматичного масштабування	0.2
4	Наявність балансування навантаження	0.4
5	Виявлення сервісів. Критерій враховує які методи використовує оркестратор для знаходження контейнерів і комунікації між ними.	0.5
6	Моніторинг. Повнота інструментів для моніторингу стану контейнерів та самого оркестратора.	0.07
7	Безпека	1
8	Здатність до роботи в динамічній архітектурі	0.8

Результати експертного оцінювання оркестраторів за пропонованими критеріями і ваговими коефіцієнтами наведені у таблиці 5.

Табл. 5. Порівняльна таблиця контейнерних оркестраторів.

Критерій	Підтр. конт.	Масшт.	Авт. масшт.	Баланс. навант.	Виявл. сервісів	Моніторинг	Безпека	Дин. арх.
Ваговий коефіцієнт	0.4	0.07	0.2	0.4	0.5	0.07	1	0.8
Засіб оркестрації								
CoreOS	1	1	1	1	1	1	1	2.75
Docker Compose	1	1	1	1	1	1	1	2.75
Docker Swarm	1	2	2	2	2	2	2	2
Kubernetes	2	2	2	2	2	2	2	0.5
Rancher	1	2	2	2	2	2	2	1.5
Nomad	4	2	2	2	2	2	2	0.5

Після проведення розрахунків, було проведено ранжування оркестраторів:

1. Docker Swarm/ Nomad (6.48)
2. Rancher (6.08)
3. Kubernetes (5.68)
4. Docker Compose / CoreOS (5.04)

За отриманими результатами, можна зробити висновок, що Docker Swarm та Nomad є найбільш підходящими оркестраторами для виконання поставленої задачі.

Висновки:

1. Враховуючи представлені вище обмеження, а саме динамічність та гетерогенність середовища, найбільш підходящими технологіями для побудови мікросервісної архітектури є containerd, Docker та Docker Swarm.

2. У подальшій роботі планується побудова гетерогенного середовища з динамічною архітектурою із залученням обчислювальних пристроїв персональних або загального користування на основі вказаних технологій.

Література

1. Смаглюк В.О., Алексєєв М.О. Використання обчислювальних потужностей мобільних пристроїв та пристроїв інтернету речей у корпоративній мережі / ПТ-2023: Збірник матеріалів конференції. К.: КПІ ім. Ігоря Сікорського, 2023. – с. 253-256
2. Mykola Alieksieiev, Volodymyr Smahliuk. Management of Life Cycle of Computing Agents with Non-deterministic Lifetime in a Kubernetes Cluster". 2023 IEEE 6th International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo). November 13 – 18, 2023.
3. Enias Cailliau, Nick Aerts. A comparative study on containers and related technologies. URL: https://www.researchgate.net/publication/320961475_A_comparative_study_on_containers_and_related_technologies (дата звернення: 20.03.2024).
4. Bibin Wilson. 16 best container orchestration tools and services. DevopsCube. URL: <https://devopscube.com/docker-container-clustering-tools/> (дата звернення: 20.03.2024).
5. Docker vs containerd vs CRI-O vs runc: which one to choose. Artkai . URL: <https://artkai.io/blog/best-containerization-tools> (дата звернення: 20.03.2024).
6. Usman Iqbal. How to choose the right container orchestrator - softwire. Softwire. URL: <https://www.softwire.com/insights/how-to-choose-the-right-container-orchestrator/> (дата звернення: 20.03.2024).
7. Yasir Rehman. Comparison of container runtimes or managment technologies [Docker, containerd, Podman, rkt]. DEV Community. URL: <https://dev.to/theyasirr/comparison-of-container-runtimes-or-managment-technologies-docker-containerd-podman-rkt-1b8b> (дата звернення: 20.03.2024).

МЕРЕЖЕВИЙ АУДИТ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖ

Ковальська Д. Д., Курдеча В.В., Якорнов Є.А.
*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна
E-mail: zashkvar.youtuba01@gmail.com*

NETWORK AUDIT OF INFORMATION COMMUNICATION NETWORKS

The need for information communication networks has grown significantly in recent years. This also means that the need for network auditing should also develop at a high speed.

Інформаційно-комунікаційний аудит є важливим інструментом для організацій для оцінки та моніторингу стану їхніх інформаційно-комунікаційних систем. У процесі аудиту оцінюється поточний стан системи, визначаються потенційні ризики, виявляються недоліки та надаються рекомендації щодо підвищення безпеки та ефективності.

Однією з головних проблем аудиту великих мереж є необхідність всебічного аналізу всієї інфраструктури для виявлення потенційних проблем, ризиків і слабких місць. Це включає перевірку конфігурацій пристроїв, аналіз трафіку, оцінку безпеки, виявлення вразливостей і перевірку відповідності стандартам і нормативним вимогам.

Крім того, великі мережі можуть мати розподілені ієрархії з різними рівнями доступу та мережевими сегментами, що ще більше ускладнює процес аудиту. [1] Координація та збір необхідної інформації з різних частин мережі вимагає значних зусиль і методів для забезпечення цілісності та надійності отриманих даних.

Проблематика сучасного інфокомунікаційного аудиту охоплює кілька аспектів, серед яких можна виділити недостатнє використання програмного забезпечення, недостатню автоматизацію процесів і занадто довгий час, необхідний для його проведення. [2]

Питання перевірки достовірності результатів аудиту є однією з найактуальніших проблем, з якими стикаються організації при проведенні телекомунікаційного аудиту. Наявність достовірної та об'єктивної інформації є ключовим елементом успішного аудиту, оскільки вона дозволяє виявити проблеми та надати рекомендації щодо подальшого вдосконалення.

Однією з основних причин проблем із точністю аудиту є людський фактор. Навіть найдосвідченіший аудитор може припуститися помилок і піддатися суб'єктивним упередженням. Інтерпретація зібраних даних і їх аналіз можуть відрізнятись залежно від досвіду, знань і особистих переконань аудитора. Це може призвести до неточних або ненадійних результатів тесту.

Удосконалення методів аудиту за допомогою програмного забезпечення ІКТ є важливим, оскільки воно може покращити процес аудиту та підвищити його ефективність. Програмне забезпечення для аудиту має ряд переваг.

Однією з головних переваг є автоматизація процесу. Це програмне забезпечення може виконувати багато рутинних завдань, пов'язаних з іспитами, наприклад: Збір даних, аналіз, відстеження завдань і звітування.[3] Це економить час і зусилля екзаменаторів і забезпечує швидку обробку інформації. Крім того, програмне забезпечення дозволяє централізовано зберігати дані, що робить їх легко доступними для аудиторів і зацікавлених сторін. Це дозволяє зручно використовувати інформацію, контролювати хід аудиту та швидко реагувати на виявлені проблеми. На рис.1 представлена модернізована модель мережевого аудиту інфокомунікаційних мереж.

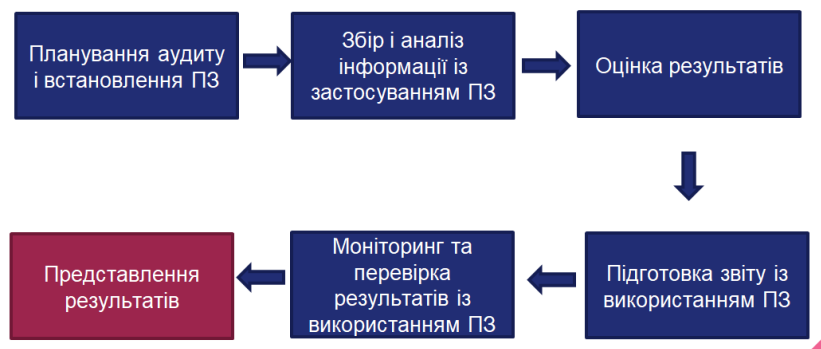


Рис.1. Модернізована модель мережевого аудиту інфокомунікаційних мереж.

У рамках дослідження було проведено два натурних випробування для порівняння ефективності двох методів аудиту. Загальний і розширений. Початкові експерименти використовували звичайні методи, включаючи ручну обробку та аналіз даних, ручні процедури тестування та інтерпретацію результатів. На рисунку 2 представлено результати проведення звичайного інфокомунікаційного аудиту без використання програмного забезпечення.

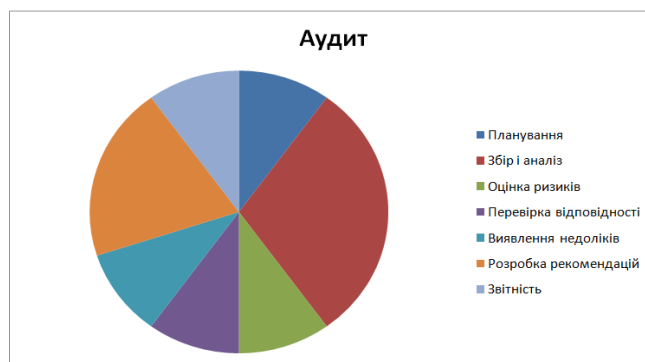


Рис.2. Результати розподілення часу при звичайному аудиті.

Автоматизований збір і обробка даних дозволяє виконувати процедури тестування швидше та ефективніше, уникаючи помилок людини та забезпечуючи послідовність результатів. Результат розподілення часу при вдосконаленому аудиті представлено на рисунку 3.

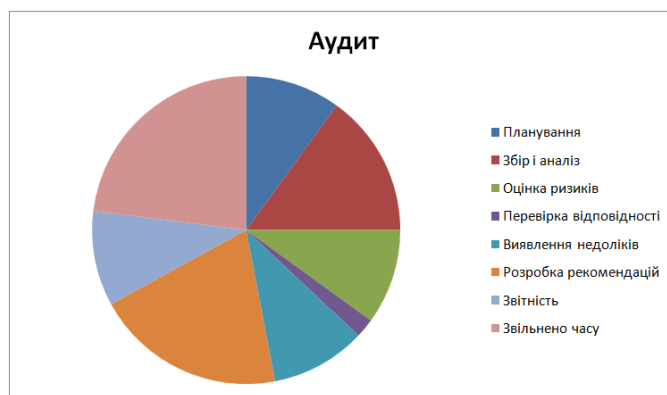


Рис.2. Результати розподілення часу при вдосконаленому аудиті.

Запровадження вдосконалених методологій аудиту в комерційне використання відкриває нові можливості для компаній для забезпечення високої якості аудиту, зниження ризику помилок і підвищення довіри клієнтів і зацікавлених сторін. Водночас важливо пам'ятати про необхідність постійного оновлення та підтримки програмного забезпечення, а також професійного навчання аудиторів, щоб максимізувати потенціал програмного забезпечення.

Модифікація стандартних методів аудиту шляхом використання програмного забезпечення є перспективним та ефективним підходом. Впровадження таких інструментів дозволяє покращити якість, точність та швидкість аудиту, а також забезпечує більш повне виявлення проблем, загроз та ризиків в інфокомунікаційних системах.

Література

1. Конахович е. Ф. Експлуатація телекомунікаційних систем. Київ : Центр учб. літ., 2019. 372 с..
2. Лунтовський А. О., Мельник І. В. Книга Комп'ютерні мережі та телекомунікації. Київ : Ун-т "Україна", 2007. 380 с.
3. Воробієнко П. П., Нікітюк Л. А., Резніченко Т. П. ТЕЛЕКОМУНІКАЦІЙНІ ТА ІНФОРМАЦІЙНІ МЕРЕЖІ. Київ : САММІТ-Кн., 210. 706 с.
4. Ковальська Д. Д. ОСОБЛИВОСТІ АУДИТУ МЕРЕЖЕВОГО ОБЛАДНАННЯ. Перспективи розвитку інформаційно-телекомунікаційних технологій та систем : Міжнар. науково-техн. конф. студентів та аспірантів, м. Київ, 12 квіт. 2022 р.
5. Ковальська Д. Д., Курдеча В. В. ПРОБЛЕМИ АУДИТУ ІНФОКОМУНІКАЦІЙНОЇ МЕРЕЖІ ВЕЛИКИХ ПІДПРИЄМСТВ. Перспективи телекомунікацій : Міжнар. науково-техн. конф. студентів та аспірантів, м. Київ, 18 квіт. 2023 р.

ПРОЦЕС ОНОВЛЕННЯ ПРИСТРОЇВ ІОТ

Терещенко В. О., Курдеча В.В.

Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: tereshenkovladislavovich2312@gmail.com

UPDATE PROCESS OF IOT DEVICES

This publication examines the main methods of updating software in IoT devices. The peculiarities of updating the software of the distributed system of the Internet of Things, which are distinguished by the steps of the update and allow to increase the efficiency of the network configuration, are considered.

Оновлення безпеки, функціональності та загальної продуктивності пристрою можна виконати кількома способами. Основні з них:

Оновлення прошивки

Оновлення мікропрограми для пристроїв ІоТ покращують вбудоване програмне забезпечення, що працює на апаратному рівні. Вони вирішують проблеми безпеки, оптимізують продуктивність та забезпечують сумісність з новими технологіями.

Оновлення програмного забезпечення

Прошивка працює на низькорівневому рівні програмного забезпечення і забезпечує базові функції та взаємодію з апаратним забезпеченням. Оновлення програмного забезпечення зазвичай зосереджені на вищих рівнях програмного стеку і включають:

1. виправлення помилок та збоїв у пз.
2. введення нових функцій для розширення можливостей пристрою.
3. удосконалення інтерфейсу користувача.

Ці оновлення забезпечують стабільну роботу пристрою та надають користувачам нові функції та поліпшення в їхньому використанні.

Автоматичне ОТА - автоматично відправляє та розгортає оновлення на підключених пристроях.

Ручне ОТА – процес оновлення керований людиною.

Блок-схема (рис. 1) ілюструє процес оновлення програмного забезпечення:

1. Ініціація: користувач або система запускає перевірку оновлень.
2. Завантаження: система завантажує та перевіряє доступне оновлення.
3. Встановлення: завантажене оновлення інсталується.
4. Завершення: система перевіряє працездатність оновлення та повідомляє користувача.

На рисунку 2, можна побачити можливі проблеми, що можуть виникнути при оновлення програмного забезпечення.

Проблеми з підключенням: для оновлення пристроїв IoT може знадобитися стабільне підключення до Інтернету. Завершення оновлень може бути складним у регіонах із поганим з'єднанням. Рішенням є очікування стабільного з'єднання або застосування ручного оновлення.

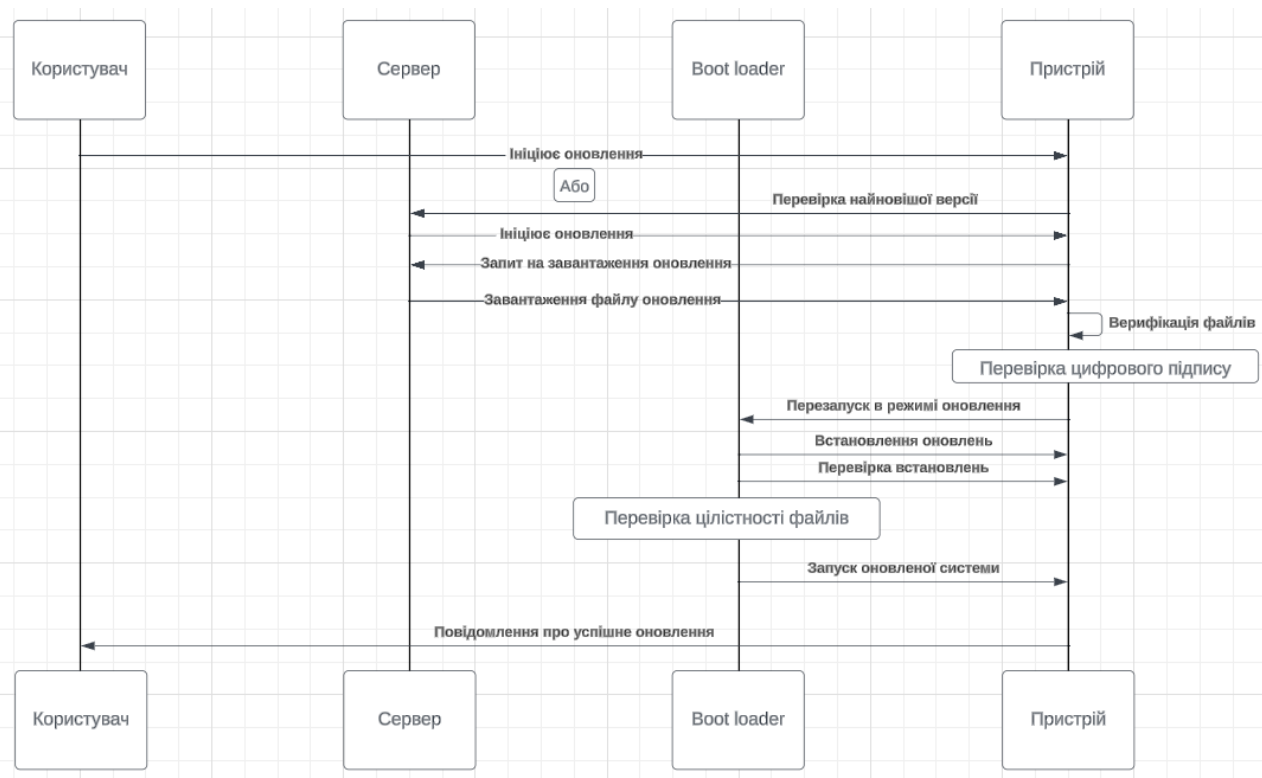


Рис. 1. Діаграма процесу оновлення пз через Boot Loader на пристрої IoT.

Пристрій зайнятий іншим завданням: загалом для цієї ситуації оновлення відбувається з пріоритизацією. Рішення – очікування відсутності активності або закінчення пріоритетного завдання.

Збій під час оновлення: Цей пункт оусоблює в собі велику кількість проблем, через які могла виникнути помилка оновлення:

1. Проблеми щодо сумісності: деякі оновлення IoT можуть бути несумісними зі старими пристроями чи певними конфігураціями, що спричиняє проблеми сумісності та функціональності.

2. Втрата даних: під час процесу оновлення існує незначна втрата даних або ризик їх пошкодження. Важливо створювати резервні копії критично важливих даних, щоб уникнути можливих випадків втрати даних.

3. Непередбачені помилки: хоча оновлення спрямовані на покращення продуктивності, час від часу вони можуть викликати нові помилки або збої, які можуть вплинути на функціональність пристрою.

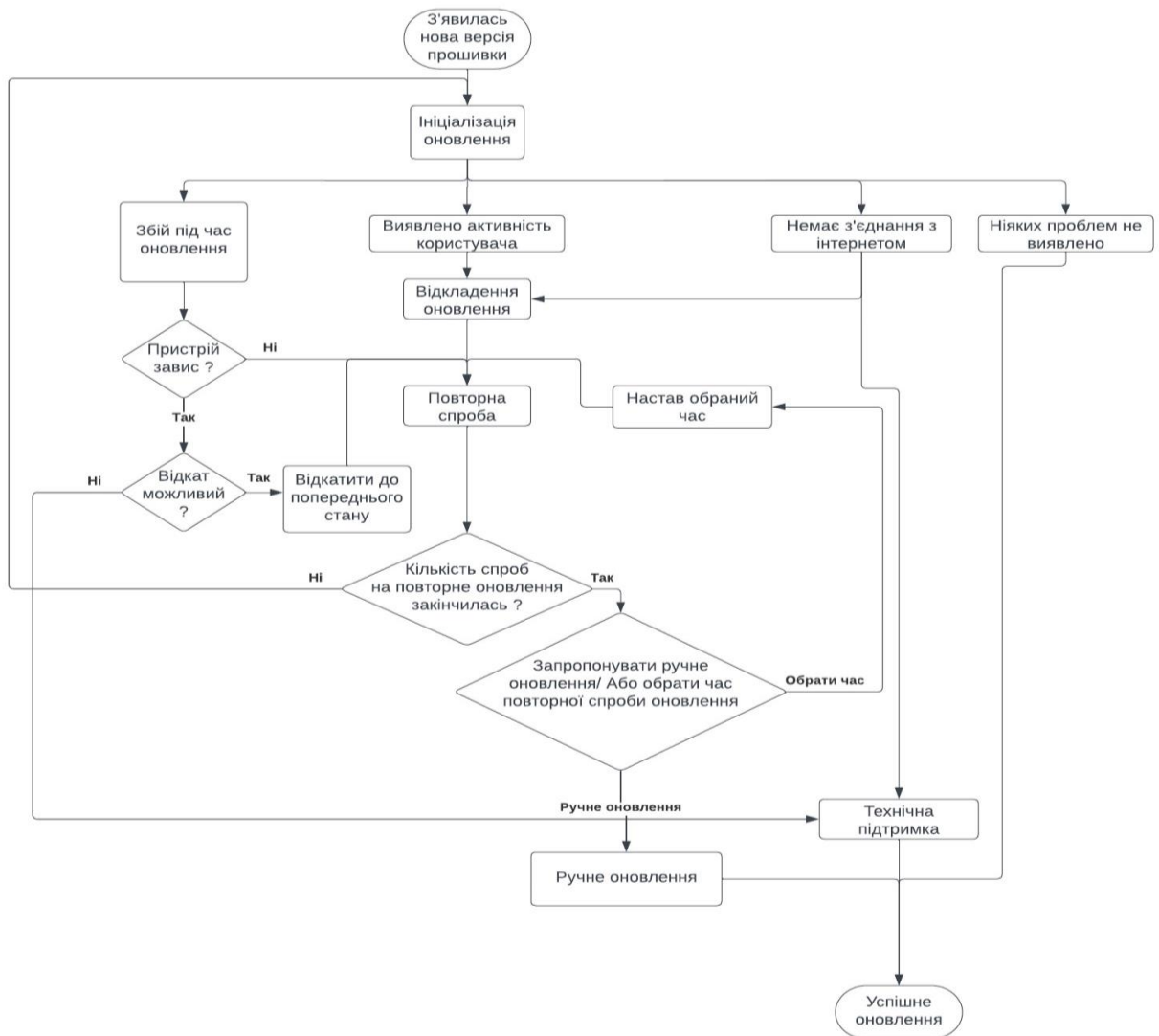


Рис. 2. Блок-схема можливих помилок та їх усунення при оновленні прошивки.

Своєчасне проектування та розробка пакету оновлень, забезпечення сумісності, проведення ретельного тестування, перевірки та усунення потенційних проблем і вразливостей, допоможуть не допустити таких помилок, і в випадку якщо все таки щось пішло не так, то якщо пристрій не зазнав критичних помилок, необхідно спробувати встановити оновлення заново, якщо відбулася помилка або якщо пристрій не може працювати справно, спробувати зробити відкат за можливості. В випадку отримання пристроєм критичної помилки, потрібно звернутися до технічної підтримки.

Література

1. J. Yamnenko, V. Kurdecha and N. Gvozdetska, "Domestic Solid Waste Disposal Logistic Optimization Using Internet of Things Technologies," 2021 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Odesa, Ukraine, 2021, pp. 1-5, doi: 10.1109/UkrMiCo52950.2021.9716596.
2. How to Update IoT Devices: Key Methods & Best Practices [Електронний ресурс] // WebbyLab. – 2024. – Режим доступу до ресурсу: <https://webbylab.com/blog/how-to-update-iot-devices/>.
3. Practical IoT: Firmware Updates [Електронний ресурс] // medium. – 2016. – Режим доступу до ресурсу: <https://medium.com/@butaji/practical-iot-firmware-updates-99568d7da15e>.

ДОСЛІДЖЕННЯ СУЧАСНИХ МЕТОДІВ ЗБОРУ ІНФОРМАЦІЇ ВУЗЛІВ ІНТЕРНЕТУ РЕЧЕЙ

Солоденко М.А., Курдеча В.В.

Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна

E-mail: *mushenok.mariia@ill.kpi.ua*

RESEARCH OF MODERN METHODS OF COLLECTING INFORMATION FROM IOT NODES

The main methods, models and technologies for collecting information in the Internet of Things (IoT) network are investigated. The generalized stages, requirements, and problems of collecting and processing information from IoT nodes using cellular networks are highlighted.

Актуальність полягає в тому, що у сучасному світі Інтернет речей (IoT) стає все більш поширеним, тож зростає кількість підключених до Інтернету пристроїв, а збір та передача інформації сприяють розвитку технологій і напряду впливають на повсякденне життя людей [1]. Попередження про погоду, нагадування про важливі події та контроль за станом побутових речей – усе це можна зробити за допомогою інформації, отриманої від сенсорів та інших пристроїв в мережі Інтернету речей. Саме тому збір та обробка інформації накладають велику відповідальність на розробників, адже неправильне використання зібраної інформації може призвести до проблем із приватністю та безпекою. Одним із можливих варіантів забезпечення зв'язку фізичних вузлів з мережею Інтернет є стільниковий Інтернет речей [2].

Основні етапи збору та обробки інформації вузлів IoT з використанням стільникових мереж представлені на рис. 1:



Рис. 1. Етапи збору та обробки інформації вузлів Інтернету речей.

Основні вимоги до збору даних в мережі IoT представлені на рис. 2 [3]:

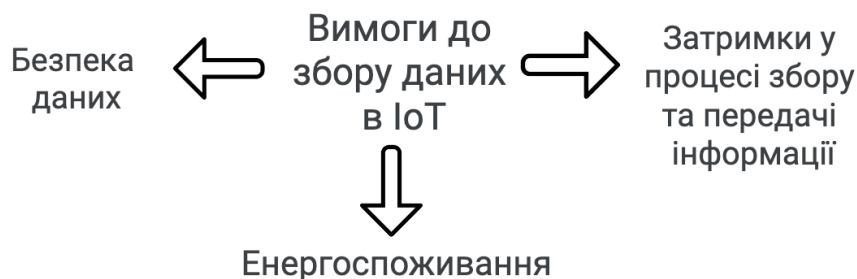


Рис. 2. Вимоги до збору даних в мережі Інтернету речей.

Перераховані вимоги досить тісно взаємопов'язані. Слід враховувати, що мережі, які передають і збирають дані з високою швидкістю, а також реалізують оптимальні моделі енергоспоживання, як правило, мають низький рівень безпеки даних.

Таблиця 1. Основні методи збору інформації в мережі Інтернету речей.

<i>Метод, модель або технологія</i>	<i>Опис</i>
Сенсорні технології	Збирають різноманітну інформацію про навколишнє середовище. Дозволяють спостерігати та вимірювати параметри у режимі реального часу. Характеризуються низькою вартістю, високою енергоефективністю та можливістю бездротового зв'язку. Приклади: температурні сенсори, сенсори вологості, руху та освітлення.
Моделі маршрутизації даних	Є основним інструментом для збору інформації вузлів Інтернету речей. Оцінюють оптимальні шляхи передачі даних між вузлами Інтернету речей. Враховують такі фактори, як швидкість, витрати, енергоспоживання та безпека. Приклади: AODV, RPL, LEACH.
Хмарні обчислювальні системи	Надають доступ до розподілених обчислювальних ресурсів через Інтернет. Дозволяють обробляти та аналізувати дані, зібрані вузлами Інтернету речей. Приклади: Amazon Web Services, Microsoft Azure, Google Cloud Platform.
Системи Fog-обчислень	Використовують обчислювальні ресурси туманних сервісів неподалік від користувачів. Забезпечують зберігання та оброблення даних в режимі реального часу. Приклади застосування: системи містобудування та управління містами.
Методи шифрування даних	Забезпечують безпеку та надійність передачі інформації в бездротових мережах Інтернету речей. Використовують легкі алгоритми шифрування для пристроїв з обмеженими ресурсами. Приклади: AES, ECC.
Проміжні платформи	Створюють інтерфейс між фізичними пристроями та програмами обробки даних. Дозволяють взаємодіяти з пристроями та реалізовувати управління інформацією. Спрощує розгортання та управління великими мережами Інтернету речей. Приклади: платформи управління містом.
Моделі соціальних мереж	Забезпечують безпеку та структуру взаємодії між пристроями Інтернету речей. Зменшують енергоспоживання та полегшують процеси збору та обробки даних. Приклади функцій: моніторинг здоров'я.

У системах стільникового IoT, інформація надходить не тільки від статичних, але також і від мобільних пристроїв, оскільки стільникові мережі IoT мають динамічну структуру.

Основні характеристиками мереж стільникового IoT (рис. 3) [4]:

- зміна структури мережі в часі;
- збільшення ймовірності помилок у мережах;
- можливість динамічного підключення та відключення пристроїв;
- складність забезпечення безпечного збору та передавання інформації.



Рис. 3. Характеристики мереж стільникового Інтернету речей.

Збір даних у стільникових мережах IoT повинен бути адаптивним до динамічних структур мереж і відповідати вимогам безпеки, обсягу споживаної енергії, швидкості відгуку та інших факторів.

Література

1. Технології інтернету речей. Навчальний посібник [Електронний ресурс]: навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології», спеціалізація «Інформаційне забезпечення робототехнічних систем» / Б. Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 12,5 Мбайт). – Київ: КПІ ім. Ігоря Сікорського, 2021. – 271 с.
2. Стільниковий IoT для безперебійного підключення // Dusun. URL: <https://dusuniot.com/uk/blog/cellular-iot-the-ultimate-guide-to-experiencing-seamless-connectivity/>.
3. УДК 621.395 DOI 10.46845/1997-3071-2021-61-105-118. О ПРОБЛЕМЕ СБОРА ДАННЫХ В СЕТЯХ ИНТЕРНЕТА ВЕЩЕЙ С ДИНАМИЧЕСКОЙ СТРУКТУРОЙ (ОБЗОР). Н. А. Жукова, А. Б. Тристанов, Тин Тун Аун, Аунг Мьо То
4. Аунг Мьо То, Аббас Саддам Ахмед, Жукова Н.А., Чернокульский В.В. Модели управления процессами сбора данных в сетях интернета вещей с динамической структурой // Computational nanotechnology. 2020. Т. 7. No 3. С. 62–71. DOI: 10.33693/2313-223X-2020-7-3-62-71.
5. U. Serhii and K. Vasyl, "Optimizing Data Transmission in IoT Networks through Enhanced Compression and Edge Computing Techniques," 2023 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Kyiv, Ukraine, 2023, pp. 76-79, doi: 10.1109/UkrMiCo61577.2023.10380347.
6. J. Yamnenko, V. Kurdecha and N. Gvozdetska, "Domestic Solid Waste Disposal Logistic Optimization Using Internet of Things Technologies," 2021 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Odesa, Ukraine, 2021, pp. 1-5, doi: 10.1109/UkrMiCo52950.2021.9716596.

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ LI-FI В МЕРЕЖІ INTERNET OF THINGS

Руденко А.А., Курдеча В.В.

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна
E-mail: anastasiarudenko078@gmail.com*

USE OF LI-FI TECHNOLOGY IN THE INTERNET OF THINGS

This work analyzed the possibilities of using Li-Fi technology in the Internet of Things network to reduce traffic in the Wi-Fi network between "smart" devices. The presented scheme of communication between devices explains the peculiarities of the interconnection of Internet of Things devices using Li-Fi technology.

За останні чотири роки кількість пристроїв Internet of Things (IoT) зросла з 8,6 мільярдів до 15,14 мільярдів[1,2]. Тому, повинні впроваджуватись нові рішення, які зможуть обслуговувати велику кількість IoT девайсів[3,4]. В середовищі, де є багато пристроїв IoT обсяг трафіку може бути дуже великим, включаючи не тільки пакети, що стосуються керування пристроями, але і службові пакети, наприклад протоколи маршрутизації. Це може значно сповільнювати передачу даних, особливо якщо цією мережею користуються мешканці будинку або працівники компанії. Також, пакети звичних нам протоколів комп'ютерної мережі розраховані на пристрої, в яких значно вище споживання електроенергії та обчислювальна здатність. Є декілька найбільш відомих технологій, що можуть вирішувати цю проблему – табл.1.

Але основна проблема, що всі ці протоколи працюють в основному в одних діапазонах радіочастот, що може вплинути на роботу як пристроїв IoT, так і інших пристроїв, що не пов'язані з цією мережею але працюють завдяки таким протоколам, наприклад, Bluetooth, наприклад навушники або аудіосистеми. Також, в великих багатоквартирних будинках може виникнути ситуація при використанні протоколів з дуже великою дальністю, що діапазону частот на всіх користувачів може не вистачити. Тому як один з варіантів можна запропонувати використання технології Li-Fi (Light Fidelity). Виходячи з попередньої моєї статті[5], можна сказати, що Li-Fi –технологія, яка може також забезпечити передачу даних в мережі IoT, але за допомогою видимого спектру світла. Li-Fi ідеально підходить для пристроїв IoT, які не переміщуються та датчики яких не зможуть бути випадковим чином перекриті, як наприклад телефон.

Основна проблема Li-Fi – складність відправки пакетів від пристрою до маршрутизатора. Для вирішення цієї проблеми можна використовувати Wi-Fi. Таким чином, ми переносимо частину трафіку з Wi-Fi мережі на Li-Fi.

Таблиця 1. Порівняння безпроводових технологій Інтернету речей.

ZigBee	Bluetooth Low Energy	Z Wave	Wi-Fi
Здатність створювати великі мережі з великою кількістю пристроїв	має високу сумісність	Простий у використанні	Високу сумісність
створений для пристроїв з низьким рівнем електроспоживання	забезпечують високу швидкість передачі даних	Мережева топологія mesh, що пристрій може дістатися до інших пристроїв у мережі через посередництво інших.	Широко представлений на ринку
Низька вартість	Може працювати на відстані до 100 метрів	Широкий спектр пристроїв	Має високу швидкість

Для цього організуємо окрему підмережу яка буде складатися з Wi-Fi маршрутизатора та окремого Li-Fi маршрутизатора, який замість радіочастотного сигналу генерувати сигнал в частоті видимого спектру, буде відповідати за комунікацію між пристроями IoT. Відправка інформації з пристроїв буде звичним нам Wi-Fi.

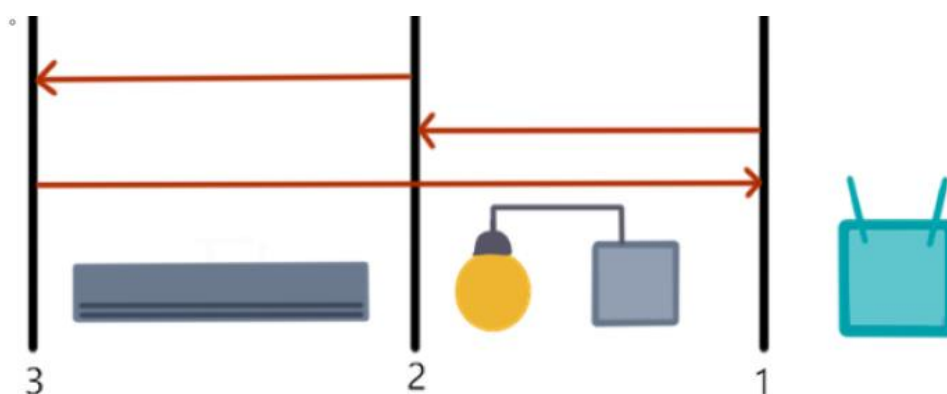


Рис. 1. Схема комунікації між пристроями, де 1- Wi-Fi маршрутизатор, 2 – Li-Fi маршрутизатор, 3 - кондиціонер та датчик температури.

Комунікація буде проводитися наступним чином: датчик температури через Wi-Fi посилає сигнал до контролера зі значенням температури, як тільки температура стала вище, ніж вказана раніше, контролер посилає команду увімкнути кондиціонер. Цей пакет досягає Wi-Fi роутера, та потім потрапляє до Li-Fi роутера та в підмережу IoT пристроїв, де за допомогою

світлового сигналу кондиціонер отримує потрібну команду та починає роботу.

Що стосується комунікації вночі, коли лампи не працюватимуть, це можливо за допомогою інфрачервоного спектру світла. Передача даних за допомогою інфрачервоного спектру електромагнітних хвиль уже давно відома завдяки Infrared Data Association (IrDA). На жаль, вдень використання інфрачервоного спектру для передачі інформації майже неможлива через завади, що створює сонце та штучні джерела освітлення.

Враховуючи все вищесказане, можна констатувати, що Li-Fi може використовуватися у поєднанні з IoT, але ця сфера вимагає більшої кількості досліджень щодо створення маршрутизатора, який зможе генерувати сигнали у видимому спектрі та економічної складової, тому що поки пристрої, що можуть підтримувати Li-Fi представлені у дуже малій кількості та вони є дуже дорогими. Але ця технологія в майбутньому, з масовим поширенням IoT пристроїв та використанням їх у звичайних будинках зможе вирішити проблему надмірної кількості трафіку між пристроями IoT у таких мережах.

Література

1. Lionel Sujay Vailshery Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030 [Електронний ресурс] 2023р. Режим доступу: URL: <https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/>
2. Globa, L., Kurdecha, V., Ushakov, S. (2023). The Modified Approach to Internet of Things Data Transmission Based on a Combined Neural Network Autoencoder. In: Dovgyi, S., Trofymchuk, O., Ustimenko, V., Globa, L. (eds) Information and Communication Technologies and Sustainable Development. ICT&SD . Lecture Notes in Networks and Systems, vol 809. Springer, Cham. https://doi.org/10.1007/978-3-031-46880-3_13
3. Ushakov Serhii and Kurdecha Vasyly, "Optimizing Data Transmission in IoT Networks through Enhanced Compression and Edge Computing Techniques," 2023 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Kyiv, Ukraine, 2023, pp. 76-79, doi: 10.1109/UkrMiCo61577.2023.10380347.
4. L. Globa, V. Kurdecha, I. Ishchenko, A. Zakharchuk and N. Kunieva, "The Intellectual IoT-System for Monitoring the Base Station Quality of Service," 2018 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Batumi, Georgia, 2018, pp. 1-5, doi: 10.1109/BlackSeaCom.2018.8433715.
5. Руденко А.А., Курдеча В.В. Порівняння технологій LI-FI та WI-FI у використанні для тепличного господарства [Електронний ресурс]/XVII МНТК"Перспективи телекомунікацій 2023"/. 2023р. Зс. Режим доступу: URL: <http://conferenc.its.kpi.ua/2023/paper/view/27607/15725>

КОМПЛЕКСНИЙ АНАЛІЗ МЕТОДІВ ВИКОРИСТАННЯ СИСТЕМ ЗБЕРІГАННЯ ЕЛЕКТРОЕНЕРГІЇ ДЛЯ MICROGRID

Степанов Г. О., Новогрудська Р. Л.

Навчально-науковий інститут телекомунікаційних

систем КПІ ім. Ігоря Сікорського, Україна

E-mail: glib4400@gmail.com

COMPREHENSIVE ANALYSIS OF METHODS OF USING ELECTRICITY STORAGE SYSTEMS FOR MICROGRID

The main data storage systems used in microgrids are considered. An analysis of different types of battery energy storage systems and their interaction with each other is carried out. The results of the analysis showed that the requirement for interoperability of such systems is not fully met and requires the formation of an ontology that will enable easy integration and autonomous operation of devices from different suppliers with different information models.

Сучасний світ швидкими кроками рухається до зникнення невідновлюваних джерел електроенергії, тому виникає нагальна потреба у використанні таких ресурсів, які можливо поновити. Сучасні мережі Microgrid пропонують недороге й екологічне рішення у вирішенні проблеми електропостачання, та забезпечують надійним джерелом регіони з нестабільною електроенергією.

З впровадженням таких мереж виникає потреба у використанні систем зберігання електроенергії, а отже необхідна і їхня інтеграція в системи керування, які розроблені для обмеженої області використання.

Система для зберігання електроенергії забезпечує своїх споживачів безперебійним доступом до живлення та має на меті знизити ймовірність втрат енергетичного ресурсу. Дані системи зберігання широко використовуються в мікромережах і можуть забезпечити плавний перехід між мережевою та ізольованою роботою мікромережі.

Велика частина розподіленої генерації (distributed generation - DG) інтегрована з акумуляторними системами зберігання енергії (battery energy storage system - BESS) у складі мікромереж, які можуть працювати як в мережевому, так і в ізольованому та комбінованому режимах. Різновидів BESS надзвичайно багато, але найпопулярніша комбінація включає в себе використання батарей та суперконденсаторів (поєднання використання накопичення та вивільнення енергії електричного поля та хімічної реакції).

Більшість мікромереж включають BESS, які можуть впливати як на стабільність, так і на надійність системи, і вони можуть використовуватися в мікромережах змінного та постійного струму [1].

Система зберігання, яка складається з акумуляторних батарей, не має належної функціональності в мікромережах у випадку високо мінливих розподілених електроенергетичних систем, таких як відновлювані джерела енергії. У цьому випадку використовують ультраконденсатори, які з точки зору щільності енергії та щільності потужності знаходяться між звичайними батареями та конденсаторами [2]. Їх встановлюють там де є дефіцит заряду від батарей.

Гібридна система зберігання енергії (hybrid energy storage system - HESS), що складається з акумуляторної батареї та ультраконденсатора, зменшує недоліки у випадку використання лише акумуляторної батареї або лише ультраконденсатора. Час заряджання/розряджання та ультраконденсатор компенсують перехідний попит протягом короткого періоду часу.

Комбінація акумуляторної батареї та ультраконденсатора обрана як гібридна система зберігання електроенергії для мікромереж (рисунок 1) з гнучким та інтелектуальним алгоритмом управління електроенергетичним споживанням.

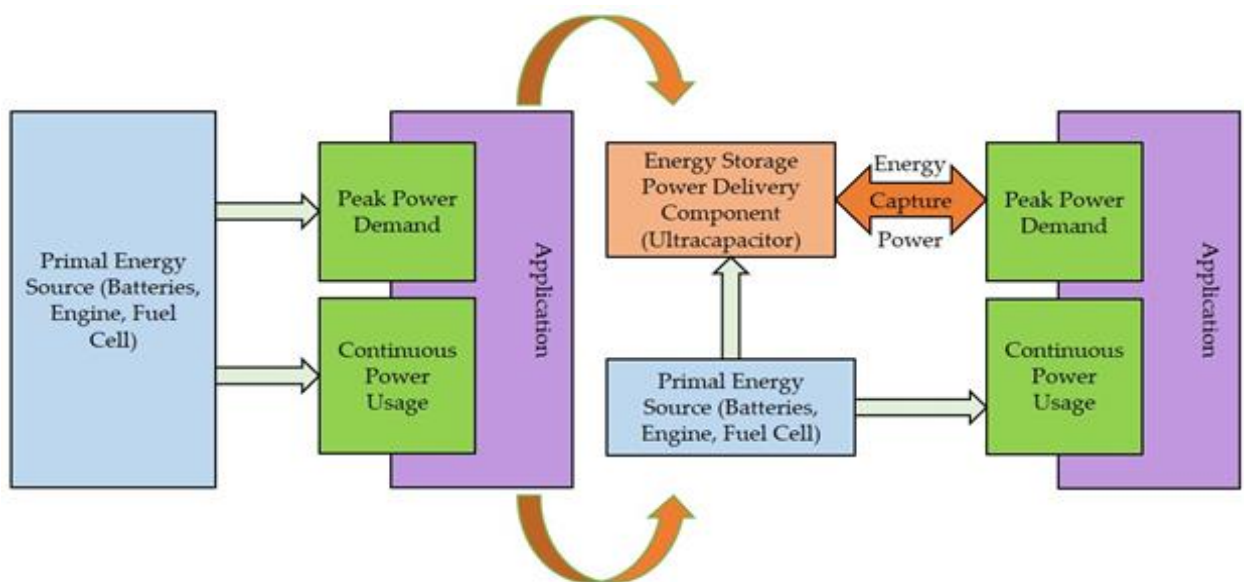


Рис. 1. Гібридна система зберігання електроенергії для мікромережі.

Батарея ініціює компенсацію згідно з алгоритмом, коли напруга на клеммах залишається в межах 0,99 і 1,01 рн (відносна одиниця). Якщо напруга має тенденцію до коливання з цієї зони (верхньої або нижньої), ультраконденсатор ініціює компенсацію.

Пік перехідного процесу, який виник у мікромережевій системі був компенсований до 1,023 pu, у випадку компенсатора тільки з акумулятором, компенсований до 1,02 pu, у випадку лише ультраконденсаторного компенсатора, і компенсований до 1,017 pu у випадку гібридної системи накопичення електроенергії як показано на рисунку 2. Отже HESS може впоратися з перехідними стрибками найбільш ефективно серед цих трьох систем [2].

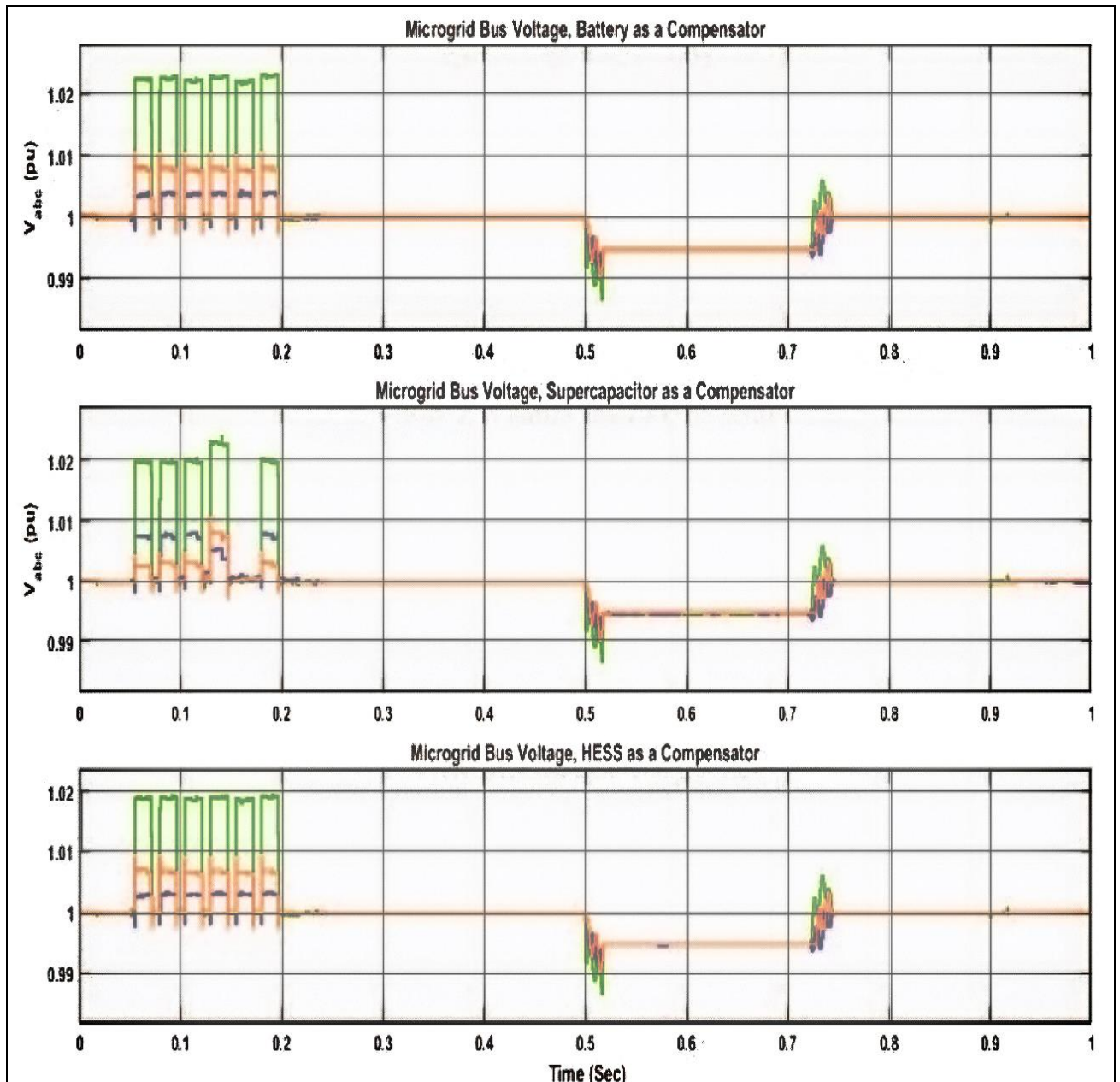


Рис. 2. Порівняння характеристик напруги на шині мікромережі між компенсатором, що працює лише на батареях, компенсатором, що працює лише на ультраконденсаторах, та компенсатором HESS.

Система керування мікромережею моделі "+" (microgrid plus control system - MPCCS), є невід'ємною частиною інтелектуальної мережі. Інтеграція MPCCS є необхідною для обміну інформацією між вузлами одного домену. Основна частина потрібних стандартів вже існує та використовується, але велика кількість з них були розроблені для інтеграції системи в обмеженій області застосування і вони не мають спільної моделі даних або спільного підходу моделювання (розглядаючи інтелектуальну мережу) [3]. Таким чином усі інтерфейси між системами які не підлягають під один стандарт потребують перетворення одного формату стандарту в інший. Так само може виникнути проблема з відображенням моделей даних якщо інтерфейс не буде підтримувати жоден з стандартів. Для рішення цієї проблеми потрібно сформулювати онтологію, за допомогою якої всі види стандартів та семантичні моделі будуть відображені на стандартній інформаційній моделі

Дана робота демонструє детальний огляд систем зберігання електроенергії які використовуватимуться для мереж Microgrid та пропонує подальший напрямок розробки онтології для формування системи управління та досягнення бажаної інтероперабельності.

Література

1. Mohamad Amin Rajabinezhad, Arman Ghaderi Baayeh, Josep M. Guerrero (2020), "Fuzzy-Based Power Management and Power Quality improvement in Microgrid using Battery Energy Storage System", 2020 10th Smart Grid Conference (SGC), P. 1-6.
2. Eklas Hossain, Ron Perez, Ramazan Bayindir (2017), "Implementation of Hybrid Energy Storage Systems to Compensate Microgrid Instability in the Presence of Constant Power Loads", International Journal of Renewable Energy Research, issue v7i2, P. 1-13.
3. Aravind Ingalalli, Ravish Kumar, Srijit Kumar Bhadra (2018), "Ontological formulation of Microgrid Control System for Interoperability", 2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA), P. 1-8.

ПІДХІД ДО БАЛАНСУВАННЯ НАВАНТАЖЕННЯ ВЕБ-СЕРВІСІВ У ГЕТЕРОГЕННОМУ КЛАСТЕРІ НА ОСНОВІ DOCKER SWARM

Сегеда С.А., Алексєєв М.О., Педан С.І.

Навчально-науковий інститут телекомунікаційних систем КІІ ім. Ігоря Сікорського, Україна

E-mail: ti71segeda@gmail.com, alexeyev@its.kpi.ua, stas.pedan@gmail.com

AN APPROACH TO WEB SERVICES LOAD BALANCING IN A HETEROGENEOUS CLUSTER BASED ON DOCKER SWARM

The work is devoted to the actual problem of effective load distribution of web services in a cluster environment. Currently, there are web services orchestration solutions in a cluster that solve this problem, but they are primarily intended for clusters with stationary architecture or for use in a cloud environment, while using as computing nodes the resources of user devices connected to the enterprise network, has advantages in terms of cost of ownership or data privacy. One of the most promising technologies that could ensure efficient functioning of the cluster in conditions of heterogeneity of working nodes and non-deterministic dynamics of architecture change is Docker Swarm, but it does not provide means of load balancing except for the cloud environment. The paper proposes an approach based on the use of Nginx load balancer to circumvent this limitation.

Робота присвячена актуальній проблемі ефективного розподілу навантаження веб-сервісів у кластерному середовищі. На даний момент існують рішення з оркестрації веб-сервісів у кластері, які вирішують цю проблему, але вони призначені насамперед для кластерів зі стаціонарною архітектурою або для використання у хмарному середовищі, у той час як використання у якості обчислювальних вузлів ресурсів користувальницьких пристроїв, підключених до корпоративної мережі, має переваги по вартості володіння або конфіденційності даних. Однією з найперспективних технологій, яка могла б забезпечити ефективне функціонування кластеру в умовах гетерогенності робочих вузлів та недетермінованої динамічності зміни архітектури це Docker Swarm, але вона не надає засобів балансування навантаження окрім як для хмарного середовища. У роботі для обходу цього обмеження пропонується підхід на основі використання балансувальника навантаження Nginx.

Кількість сервісів в Інтернеті зростає, тому проблема збільшення продуктивності серверів, які їх обслуговують, є актуальною. Цю проблему зазвичай вирішують на основі хмарних рішень, які дозволяють побудувати кластер серверів майже будь якої потужності, який буде автоматично масштабуватись, виходячи з поточних потреб. Але в умовах, коли у наявності компаній є обчислювальні пристрої, підключені до корпоративної мережі, доцільним може бути залучення простоюючих ресурсів таких пристроїв: це не потребує додаткових інвестицій і в організаціях є в наявності багато обладнання - персональні комп'ютери, пристрої "розумного дому" та

інтернету речей які не потребують автономності роботи та простоюють. У попередній роботі [1] було показано, що однією з перспективних технологій, яка могла б забезпечити ефективне функціонування кластера в умовах гетерогенності зазначених робочих вузлів та очевидної недетермінованої динамічності зміни архітектури кластера, побудованого із залученням таких ресурсів є Docker Swarm, але вона має засоби балансування навантаження тільки для хмарного середовища [2]

Отже, у роботі поставлена задача ефективного балансування навантаження веб-сервісів у кластері під керуванням Docker Swarm, побудованому на основі незадіяних ресурсів пристроїв, підключених до корпоративної мережі.

Типовою архітектурою сучасного серверу може розглядатись наступна [2]: в нас існує кластер (сервер), який реалізує бізнес логіку і обслуговує застосунок. Для того, щоб запити могли потрапити всередину сервера необхідний балансувальник навантаження, наприклад Nginx або Apache HTTP Server [3]. Все, що робить балансувальник у більшості випадків, це перенаправляє запит у вказане місце, тобто в нашому випадку, на сервер з бізнес логікою. Проте, сервер може бути не один і балансувальник може розподілити запити між ними за заданим алгоритмом.

В даній роботі запропоновано використовувати алгоритм “Round Robin”. При цьому кожен сервер має свою “вагу” і запити розподіляються відповідно до неї [3].

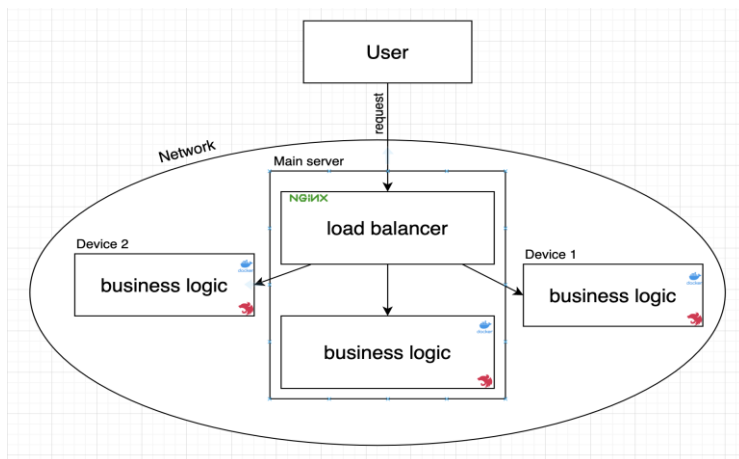


Рис.1. Структурна схема проекту.

Для вирішення поставленої задачі у роботі пропонується архітектура, показана на рис.1. - це мережа, в якій знаходиться головний сервер, в якому в свою чергу знаходиться балансувальник та бізнес логіка, упакована в Docker контейнер. Всі комп'ютери які планується застосувати, також мають встановлений Docker і знаходяться в одній мережі з головним сервером, хоча останнє і не є обов'язковим.

Docker зручно використовувати для контейнеризації застосунку, бо він дозволяє абстрагуватися від операційної системи, на якій буде запущено додаток, а також дозволяє запакувати все в образ, який потім може бути скачаний з репозиторія для їх зберігання, такого як Docker Hub або AWS ECR. При запуску головний сервер публікує посилання на певній адресі, перейшовши за яким починається завантаження скрипта, який після виконання скачує образ зі схожою бізнес логікою, встановить його та запустить. Бізнес логіка в свою чергу звертається в балансувальник з певним

запитом. Для того щоб обробити цей запит у даній роботі використано CGI. CGI має певні переваги над іншими методами для зміни конфігурації під час роботи - це програмне рішення, яке не використовує багато системних ресурсів, не потребує сторонніх технологій, функціоналу яких буде забагато для цих цілей, має багато варіантів реалізації на різних мовах програмування та не потребує багато зусиль в розробці []. Отримуючи запит, ми маємо ір адресу комп'ютера з якого цей запит було отримано і додаємо його до списку серверів, на які запити будуть транслюватися в подальшому.

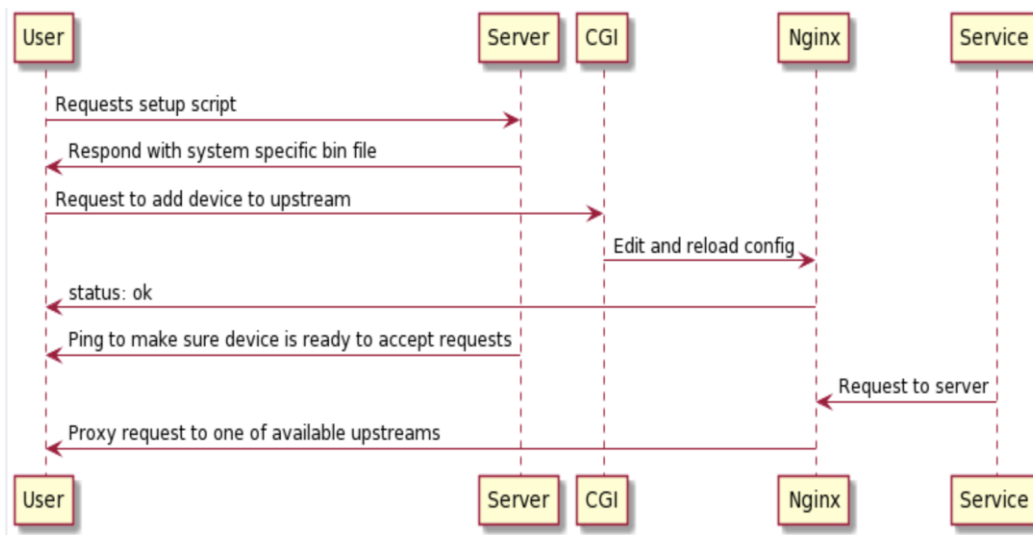


Рис. 2. Діаграма станів проекту.

Після цього необхідно лише перезавантажити конфігурацію і подальші запити будуть розподілятися між серверами.

Висновок. Запропоноване рішення легке у розробці, швидкодіюче, гнучке у налаштуванні та здатне вирішити поставлену задачу – збалансувати навантаження між контейнеризованими сервісами у кластері під керуванням Docker Swarm, побудованому на основі неадіяних ресурсів пристроїв, підключених до корпоративної мережі.

Література

1. Swarm mode key concepts. URL: <https://docs.docker.com/engine/swarm/key-concepts/#load-balancing> (дата звернення: 20.03.2024).
2. Шелест Є.В., Алексєєв М.О., Педан С.І. Оглядний аналіз технологій контейнеризації для використання у гетерогенному середовищі із динамічною архітектурою / ПТ-2024: Збірник матеріалів конференції. К.: КПІ ім. Ігоря Сікорського, 2024.
3. Tony Mauro of F5, "Choosing an NGINX Plus Load-Balancing Technique", October 29, 2015, URL: <https://www.nginx.com/blog/choosing-nginx-plus-load-balancing-techniques> (дата звернення: 20.03.2024).

РОЗРОБКА ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ ДЛЯ АВТОМАТИЗАЦІЇ МОНІТОРИНГУ ТА УПРАВЛІННЯ ТРАНСПОРТНОЮ СИСТЕМОЮ МІСТА КИЄВА З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Столяр С.В., Комаров І.Ю., Ігнатова С.С.
*Політехнічний ліцей КПІ ім. Ігоря Сікорського,
Комунальний заклад позашкільної освіти
«Київська Мала академія наук учнівської молоді», Україна
E-mail: plkpi_kvnt@ukr.net*

Проект з дослідження сфери інфраструктури у місті Києві та впровадження сучасних технологій для оптимізації транспортної системи. Запропонована модель з урахуванням ефективності та вартості, розглянуто переваги та способи застосування. Проект відповідає запитам сучасного розвитку міста та може сприяти більшій мобільності населення, підвищенню безпеки дорожнього руху, зменшенню економічних втрат і вирішенню екологічної проблеми, пов'язаної з якістю повітря. Експеримент був проведений за допомогою незначних ресурсів, щоб запропонувати розв'язання масштабних проблем з корками у місті Києві.

DEVELOPMENT OF AN INTELLIGENT SYSTEM FOR AUTOMATING THE MONITORING AND MANAGEMENT OF THE TRANSPORT SYSTEM OF THE CITY OF KYIV USING ARTIFICIAL INTELLIGENCE

A project to study the infrastructure sector in Kyiv and introduce modern technologies to optimize the transport system. A model is proposed, taking into account efficiency and cost, and the advantages and method of application are considered. The project meets the needs of modern city development and can contribute to greater mobility of the population, improve road safety, reduce economic losses and solve the environmental problem related to air quality. The experiment was conducted with few resources to propose a solution to the large-scale traffic jam problems in Kyiv.

Сучасний Київ, який стрімко розвивається та стикається зі збільшенням кількості автотранспорту, потребує інноваційних рішень для транспортної інфраструктури. Збільшення кількості автомобілів, неконтрольований масштаб трафіку та аварійна інфраструктура призводять до заторів, особливо на мостах між лівим та правим берегами Дніпра та на виїзді з міста. У креативному вирішенні цих викликів необхідно враховувати, що просте збільшення кількості маршрутів може призвести до переваги автомобільного транспорту та втрати гуманістичного аспекту міського планування. Замість того, щоб зосереджуватися виключно на розширенні мережі транспортних комунікацій, можна розглянути більш раціональний та бюджетний метод. Наприклад, впровадження інтелектуальних систем управління та моніторингу. Використання передових технологій штучного інтелекту дозволить не лише ефективно прогнозувати та оптимізувати трафік, а й створити більш комфортні та безпечні умови для киян. У

майбутньому розумне управління транспортними системами максимізує потенціал чинної мережі пересування та зменшить потребу в постійному розширенні автомагістралей. Такий підхід не лише допоможе розв'язати актуальні транспортні проблеми, але й сприятиме створенню екологічно чистого міського середовища.

У рамках реалізації даного проєкту, який спрямований на створення інтелектуальної системи управління транспортною системою міста Києва, передбачається не лише поліпшення мобільності та загальної якості життя мешканців, але й значне зменшення економічних втрат, пов'язаних з транспортними заторами та неефективним управлінням рухом.

Мета роботи – за допомогою штучного інтелекту зменшити затори на експериментальному прототипі перехрестя, щоб у майбутньому впровадити у транспортну систему Києва. Актуальність цього дослідження обумовлена необхідністю впровадження інноваційних та раціональних підходів в управління транспортною мережею Києва з метою її ефективного покращення та відповіді на сучасні виклики міської мобільності.

Традиційні системи не враховують фактор кількості транспортних засобів на дорозі в певний момент часу. Недоліком таких систем є те, що вони не можуть налаштовувати тривалість зеленого сигналу в залежності від поточних умов дорожнього руху. Це може призвести до заторів на перехрестях, де тривалість зеленого сигналу недостатня для того, щоб звільнити смуги з інтенсивним рухом. Потрібно змінити цю ситуацію та мінімізувати проведений автомобілями час в очікуванні своєї черги проїхати. Створення нової моделі допоможе вирішити яка смуга потребує більшої тривалості зеленого сигналу на основі кількості автомобілів у смузі, а не фіксованої тривалості. Ця модель також допоможе зменшити втрати часу на дорогах, де менше автомобілів, і використати цей час для інших завантажених доріг. Для створення цієї моделі використовувався модуль NumPy і навчання нейронної мережі на реальних даних зі звіту про трафік на київському проспекті Леся Курбаса. Для того, щоб нейронна мережа ефективно виконувала поставлену перед нею задачу, потрібно перевіряти правильність її роботи. Це зроблено з використанням навичок програмування, а саме створення коду для побудови лінійної регресії та візуалізації результатів за допомогою бібліотек NumPy, Pandas, Matplotlib і scikit-learn. Скрипт будує лінійну регресійну модель для передбачення часу зеленого світла на основі відсоткової кількості автомобілів. Код охоплює розподіл даних на навчальні та тестові набори, побудову та навчання моделі лінійної регресії, оцінку точності моделі та візуалізацію результатів.

На рисунках 1 та 2 видно помітну різницю ефективності роботи класичної та експериментальної систем. Рис. 1 демонструє, що час нераціонально використовується: три завантажені смуги чекають, поки зелене світло горить на смузі, де не їде жодна машина. Це може призводити до зайвого очікування та заторів. На рисунку 2 зображено динамічне управління світлофорами, де зелене світло не вмикається, якщо на смузі немає автомобілів. Це дозволяє ефективно використовувати час світлофорів

та підтримувати плавний рух транспорту. Враховуючи інформацію про кількість машин та навантаженість, наявна транспортна система зможе легко змінювати рух автомобілів для оптимізації потоку транспорту та уникнення заторів.



Рис. 1. До.



Рис. 2. Після.

На основі аналізу було розроблено проєкт інтелектуальної системи для автоматизації моніторингу та управління транспортною системою Києва. В результаті тестування було виявлено, що система дозволила усунути затори та збільшити швидкість руху автомобілів на експериментальній моделі. Дослідження довело, що за допомогою незначних ресурсів можна створити експериментальний прототип, що зміг би скоротити економічні втрати, зменшити викиди парникових газів та забезпечити пересування водіїв. Основними ризиками та слабкою стороною даної моделі є ШІ, який має недосконалу точність та залежний від даних на яких навчався. Але якщо взяти до уваги всі ці аспекти його роботи та встановити нормативні рамки, можна уникнути цих ризиків.

Література

1. Гайд про управління дорожнім рухом за допомогою ШІ [Електронний ресурс]. - Режим доступу: <https://www.ijert.org/research/using-ai-and-machine-learning-techniques-for-traffic-signal-control-management-review-IJERTV6IS110065.pdf>
2. Документація про бібліотеку NumPy [Електронний ресурс]. – Режим доступу: <https://numpy.org/doc/stable/>
3. Гайд по бібліотеці Pygame [Електронний ресурс]. – Режим доступу: <https://riptutorial.com/pygame/example/16814/installing-pygame>
4. Гайд зі створення лінійних регресій [Електронний ресурс]. – Режим доступу: <https://robotdreams.cc/uk/blog/437-shcho-take-liniyna-regresiya>
5. Отриманні дані для навчання нейронної мережі [Електронний ресурс]. – Режим доступу: <https://mtu.gov.ua>

Keywords: TRAFFIC JAMS, TRANSPORTATION SYSTEM, KYIV, TRAFFIC, MODERN TECHNOLOGIES, TRAFFIC LIGHT CONTROL, MACHINE LEARNING.

Ключові слова: КОРКИ, ТРАНСПОРТНА СИСТЕМА, КИЇВ, ДОРОЖНІЙ РУХ, СУЧАСНІ ТЕХНОЛОГІЇ, УПРАВЛІННЯ СВІТЛОФОРАМИ, МАШИННЕ НАВЧАННЯ.

TELEGRAM - БОТ ДЛЯ РОЗРАХУНКУ ПОДАТКІВ

Радіонов М.Р., Комаров І.Ю., Ігнатова С.С.
*Політехнічний ліцей КПІ ім. Ігоря Сікорського,
Комунальний заклад позашкільної освіти
«Київська Мала академія наук учнівської молоді», Україна
E-mail: plkpi_kvnt@ukr.net*

Проект ставить за мету розробку та впровадження телеграм-бота, спрямованого на автоматизацію процесу розрахунку податків. З врахуванням актуальності цієї теми у сучасному світі та з врахуванням широкого застосування месенджера Telegram, обраний підхід обіцяє створення інноваційного інструменту для спрощення складних фінансових обчислень для користувачів різного роду. Одним з ключових аспектів дослідження є програмування, тестування та валідація розробленого бота.

TELEGRAM - TAX CALCULATION BOT

The project aims to develop and implement a Telegram bot aimed at automating the tax calculation process. Taking into account the relevance of this topic in the modern world and taking into account the widespread use of the Telegram messenger, the chosen approach promises to create an innovative tool for simplifying complex financial calculations for users of all kinds. One of the key aspects of the research is the programming, testing and validation of the developed bot.

Податки є невіддільною частиною сучасної економіки. Вони використовуються для фінансування державних витрат, забезпечення соціальних програм і підтримки економічного зростання. Розрахунок податків є складним процесом, який вимагає знань і досвіду. У сучасних умовах все більш популярними стають автоматизовані системи розрахунку податків. Вони дозволяють підвищити ефективність і точність розрахунків, а також спростити процес для користувачів. Одним із варіантів автоматизованої системи розрахунку податків є Telegram-бот. Telegram-боти є популярним інструментом, який використовується для різних цілей, включаючи надання інформації, розваги й автоматизацію завдань.

В роботі проаналізовано потреби користувачів у сфері розрахунків податків та визначено ключові функціональні вимоги до бота. Особлива увага приділяється вивченню технічної архітектури проекту, включаючи вибір мови програмування, організацію взаємодії з Telegram API, та вибір

системи управління базою даних. За допомогою мови програмування Python та бібліотеки python-telegram-bot реалізовано модульну структуру, забезпечуючи читабельність та ефективність коду. Автоматизоване тестування включає різні сценарії введення користувача, а також тестування стійкості до помилок.

Однією з інноваційних частин проєкту є гнучкість та масштабованість бази даних. Використання SQL-запитів дозволяє розширювати функціонал бази даних без внесення суттєвих змін у вихідний код, що важливо для легкої адаптації до нових вимог. Створений телеграм бот став ефективним інструментом для автоматизації розрахунків податків, що значно спрощує цей процес та робить його більш зручним для користувача. Розробка бота допомогла розкрити важливі аспекти програмування, такі як обробка даних, робота з API та інтеграція з месенджером.

Література

1. Які є види податків? Системи оподаткування. Веб – сайт. URL: <https://online.novaposhta.education/blog/pro-yaki-vidi-podatktiv-neobhidno-znati-pidpriyemtsyam-v-ukrayini>
2. Загальнодержавні податки. Веб – сайт. URL: <https://tax.gov.ua/zakonodavstvo/podatki-ta-zbori/zagalnoderjavni-podatki/>
3. Документація по мові Python [Електронний ресурс]. – Режим доступу: <https://pythonguide.rozh2sch.org.ua/>
4. Офіційний сайт мови програмування Python [Електронний ресурс]. – Режим доступу: <https://www.python.org/>
5. Офіційний сайт середовище розробки PyCharm [Електронний ресурс]. – Режим доступу: <https://www.jetbrains.com/pycharm/>
6. Як підключити базу даних до Telegram – боту на YouTube: <https://youtu.be/b0Dplx4M5zg?si=-CDRsc4KqEqVScJp>

Ключові слова: TELEGRAM - БОТ, БАЗА ДАНИХ (БД), ПОДАТКИ, PYTHON, SQLITE3, TELEGRAM API

ВИЯВЛЕННЯ СИГНАЛІВ БПЛА ЗА ДОПОМОГОЮ НЕЙРОМЕРЕЖ (НА ПРИКЛАДІ НАБОРІВ ДАНИХ КОМЕРЦІЙНИХ ДРОНІВ)

Чубай Д. Р., Ігнатова С.С.

Київська інженерна гімназія, Комунальний заклад позашкільної освіти «Київська Мала академія наук учнівської молоді»

E-mail: daniil.chubay@gmail.com

DETECTION OF UAV SIGNALS USING NEURAL NETWORKS (USING THE DATA SETS OF COMMERCIAL DRONES)

The article describes the features of communication protocols in different UAVs and proposes to use neural networks to detect and classify UAV signals. During the research, it was found that CNN models score the best at the detection/classification of UAVs. RNN and Transformer models showed abnormal results.

З розвитком застосування БПЛА у військовій та цивільній сферах зростає потреба у засобах виявлення безпілотників. Ефективні засоби виявлення БПЛА допомагають військовослужбовцям мати краще уявлення про стан справ у повітряному просторі, тому дослідження з цієї теми можуть спасти життя наших воїнів та загалом покращити безпеку людей.

У різних БПЛА використовують різні види протоколів зв'язку. В них, зокрема, використовуються різні види модуляції. В залежності від типу інформації, яка передається, модуляції поділяються на цифрові та аналогові.

У цифрових модуляціях в БПЛА переважно використовуються технології псевдовипадкового перелаштування робочої частоти та ортогонального частотного поділу каналів. Ортогональний частотний поділ каналів (ОЧПК; англ. Orthogonal Frequency-Division Multiplexing — OFDM) – це різновид частотного поділу каналів, який модулює цифрові дані різними близькими несучими хвилями. До протоколів ОЧПК, які використовуються в БПЛА, належить WI-FI стандартів 802.11n або 802.11ac, Enhanced WI-FI, розроблений компанією DJI. ОЧПК використовується у дронах Yuneec Mantis Q, Parrot ANAFI, DJI Mavic Air. Іншою технологією, яка поширена в БПЛА, є псевдовипадкове перелаштування робочої частоти (ППРЧ; англ. Frequency-Hopping Spread Spectrum) – метод передачі радіосигналів шляхом швидкої зміни несучої сигналу. DJI має свої протоколи, засновані на ППРЧ, зокрема Lightbridge, Ocusync. У популярному приймачі FrSky теж використовується FHSS [5, с. 12]. Окрім того, до цифрових протоколів належать сімейство DSM (зокрема, DSMX, DSM2, DSSS), ACCESS/FRSKY, A-FHSS, AFHDS та AFHDS2, HiSky, DEVO [3, с. 177–178]. В БПЛА може використовуватися стільниковий зв'язок 3/4G. Для навігації використовують зв'язок GPS (GNSS), зокрема за допомогою протоколу NMEA [8, с. 35-37]. Окрім цифрової, використовується аналогова модуляція. Зокрема, в стандартах PAL, NTSC. Для контролю БПЛА може використовуватися FM модуляція [3, с. 176]. БПЛА/дрони можуть

використовувати частоти 27, 28, 35, 40, 220–400, 433, 725–770, 790–830, 850–916, 935–960, 950–1200 МГц, 1.4–1.85, 2.1–2.7, 4.4–5.85, 14.4–14.83, 15.15–15.35, 17.1–18.8, 21.1–21.7 ГГц, [2, с. 32–33][1, с. 18–19][3, с. 179–180]. Сюди входять частоти, на яких здійснюється контроль БПЛА, навігація, передача телеметрії, передача відео тощо. Отже, в технологіях комунікації у БПЛА маємо досить велике різноманіття.

Машинне навчання в останні роки стало популярним та ефективним інструментом для автоматизації складних задач. На відміну від класичних алгоритмів, нейронні мережі здатні за допомогою проб і помилок виявляти комплексні структури, комбінації різних параметрів. Зокрема, вони здатні вирішувати задачі, пов'язані з класифікацією сигналів [6, с. 451–460]. Отже за допомогою нейромереж можна й виявляти різні види БПЛА за їх радіосигналами. Як вже було зазначено, різні види та моделі БПЛА мають різні технології та протоколи комунікації, через що вручну описувати алгоритм виявлення кожного окремого пристрою є неефективним способом. Натомість нейромережі можуть самі виокремлювати параметри, за якими треба визначати присутність сигналів БПЛА. Наприклад, присутність БПЛА може бути виявлена нейромережами внаслідок відстеження того, наскільки часто передаються пакети даних на певних частотах. Тому ми вирішили дослідити які моделі нейромереж найбільш ефективні у виявленні/класифікації БПЛА.

Для цього ми використовували набори даних з записами радіосигналів дронів, доступні у вільному доступі. Спочатку нами було обрано набір даних «DroneRF». Втім через велику кількість відліків (2 млн на кожному сегменті) тренування моделей нейромереж на цьому наборі даних займало забагато часу. Тому ми вирішили звернутися до набору даних «Noisy Drone RF signals classification».

Для класифікації сигналів нами було обрано протестувати згорткові нейронні мережі, рекурентні нейронні мережі і моделі-трансформери, оскільки ці моделі непогано себе показали у схожих галузях. Згорткові нейронні мережі (ЗНН; англ. Convolutional neural network – CNN) різняться від інших нейронних мереж наявністю згорткових шарів, які мають ядро-фільтр, що проходиться по масиву вхідних даних. Ми використали модель нейромережі, запропоновану в [10], додавши до неї шар виключення. В результаті було отримано точність класифікації на перевірочних даних 86% (див. рис. 1).

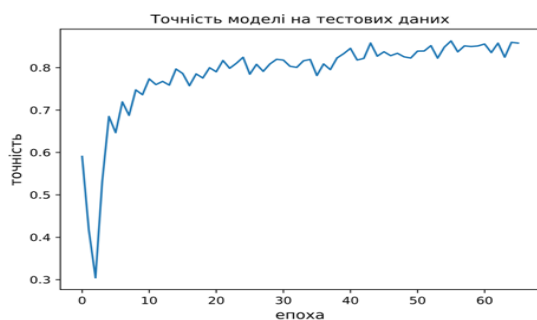


Рис. 1. Точність моделі ЗНН.

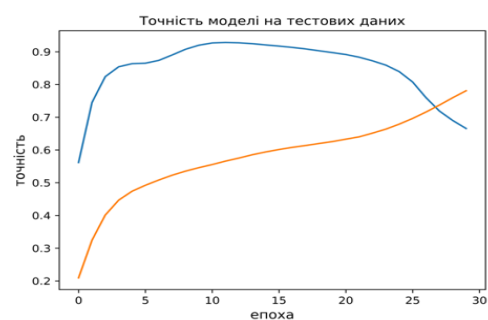


Рис. 2. Точність моделі РНН.

Класифікація спектрограм не дала помітних кращих результатів: було отримано точність лише 62%. Наступним видом нейронних мереж, який ми спробували застосувати, були рекурентні нейронні мережі (РНН; англ. recurrent

neural network — RNN). Їх особливість полягає в тому, що вони оброблюють послідовності даних з зберіганням внутрішньої пам'яті. У більшості випадків РНН вже в першій епосі досягала точності на перевірочних даних близько 95%, але згодом точність дуже різко падала. Найбільш реалістичні результати були отримані, коли коефіцієнт навчання (параметр `learning_rate`) був понижений до значення 10^{-6} (див. рис. 2). Були також розглянуті трансформери – нові моделі нейромереж, описані в 2017 р. у статті „Attention is All You Need”. Для нашої задачі ми використали імплементацію, запропоновану в [7] для класифікації часових рядів, але змінювали там коефіцієнт навчання та значення параметру `dropout`. Трансформер вів себе подібно до рекурентних нейронних мереж.

Отже, найкраще у виявленні/класифікації дронів себе показали згорткові нейронні мережі з точністю 86%. Навчання рекурентних нейронних мереж та трансформерів дало аномальні результати. Можливо проблема полягає у поганій сумісності цих моделей нейромереж з обраними наборами даних.

Напрямами нашої подальшої роботи буде: написання кращої попередньої обробки та виділення ознак у наборах даних; імплементація нейронної мережі з підкріпленням (для динамічного корегування ваг нейронної мережі на основі нових записів); розробка пристрою, який аналізуватиме спектр на наявність БПЛА у режимі реального часу. Останнє може здійснюватися за допомогою SDR приймача. Для вивантаження нейромережі на пристрої з обмеженими обчислювальними можливостями існує бібліотека Tensorflow Lite Micro (TFLM). Прикладом імплементації зв'язки SDR (HackRF), TFLM і Keras є система для аналізу радіосигналу криптогаманця Ledger Blue, яку розробили Т. Рот та ін. [9].

Література

1. Боротьба з безпілотними літальними апаратами (за досвідом проведення ООС (раніше АТО). К.: «Центр учбової літератури», 2022. 43 с.
2. Макаренко С. И. Противодействие беспилотным летательным аппаратам. СПб.: Наукоемкие технологии, 2020. 204 с.
3. Communication, Remote Control and Autonomous Flights. Unmanned electrical vehicles and autonomous system simulation / Editors: Sell R., Czekalski P., Nıkitenko A. Riga: RTU Press, 2021. pp. 175-181.
4. Noisy Drone RF Signal Classification. Kaggle. URL: <https://www.kaggle.com/datasets/sgluege/noisy-drone-rf-signal-classification>
5. Rozenbeek D. J. Evaluation of Drone Neutralization Methods using Radio Jamming and Spoofing Techniques. 2020. URL: <https://www.diva-portal.org/smash/get/diva2:1460807/FULLTEXT01.pdf>.
6. Steven W. S. The Scientist & Engineer's Guide to Digital Signal Processing. California: California Technical Pub, 1999. 640 p.
7. Timeseries classification with a Transformer model. Keras. URL: https://keras.io/examples/timeseries/timeseries_classification_transformer/
8. UAV Networks and Communications / Edited by Kamesh Namuduri, Serge Chaumette, Jae H. Kim, James P. G. Sterbenz. Cambridge University Press, 2018. 242 p.
9. Using TensorFlow / machine learning for automated RF side-channel attack classification. Leveldown security. URL: <https://leveldown.de/blog/tensorflow-sidechannel-analysis/>.
10. Zhiguang Wang, Weizhong Yan, Tim Oates. Time Series Classification from Scratch with Deep Neural Networks: A Strong Baseline. arXiv. URL: <https://arxiv.org/abs/1611.06455>.

THE ROLE OF ARTIFICIAL INTELLIGENCE IN THE FORMATION OF WIRELESS NETWORKS

¹Oliinyk D.I., ²Nizhnyi 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@lil.kpi.ua

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ У ФОРМУВАННІ БЕЗДРОТОВИХ МЕРЕЖ

У статті наводиться аналіз розвитку технологій Інтернету речей (*IoT*) та їх інтеграції з штучним інтелектом (*III*), а також розглядаються майбутні напрямки використання цих технологій, зокрема в контексті бездротових мереж 5G та 6G. Встановлено, що майбутні мережі еволюціонуватимуть до інтеграції різних середовищ (космос, повітря, земля, море) та впровадження нових послуг, таких як масові комунікації машинного типу (*mMTC*), зв'язок з наднадійністю та низькою затримкою (*uRLLC*) і розширений мобільний широкопasmовий зв'язок (*eMBB*).

The article provides an analysis of the development of Internet of Things (IoT) technologies and their integration with artificial intelligence (AI), as well as considers future directions for the use of these technologies, particularly in the context of 5G and 6G wireless networks. It is established that future networks will evolve to integrate different environments (space, air, land, sea) and introduce new services such as mass machine-type communications (mMTC), ultra-reliability and low-latency communications (uRLLC) and advanced mobile broadband communication (eMBB).

The Internet of Things (*IoT*) has created the need for massive connectivity for billions of devices that require system power far beyond the needs of current networks and the introduction of an efficient communication paradigm. Artificial intelligence (AI) technologies, which are equivalent to human intelligence based on machine learning systems, are now being integrated into all spheres of human activity. These have already found their implementation in self-driving car navigation, face recognition, language processing, logical reasoning, etc. Future research includes: augmented reality; autonomous *IoT* industry; digital doubles; the formation of the Metaverse, etc. [1]. There is a consensus in the research community that future networks will evolve towards the integration of space, air, land and sea, providing communication services with wide coverage [2]. Wireless networks of the future, particularly artificial intelligence-based 5G and 6G, are seen as the standard technology for cellular wireless networks. Massive machine-type communications (*mMTC*) are becoming the main driver to realize the vision of a scalable IoT with heterogeneous applications with mass access of telecommunications consumers. Thus, *mMTC* with ultra-reliability and low-latency communication (*uRLLC*) and enhanced mobile broadband (*eMBB*) form new types

of diversified services in future networks.

Despite the development of 5G in recent years, the fifth generation of cellular technology still poses some challenges due to both wavelength limitations and cost debates. Data centers are already facing changes caused by wireless networks, such as: virtualization, programmable networks, edge computing, and the challenges of simultaneously supporting public and private networks. 5G and 6G technologies are expected to make greater use of the distributed radio access network (*RAN*) and terahertz spectrum to increase bandwidth, reduce latency and improve spectrum sharing.

RAN networks were once proposed to effectively reduce capital and operational costs and optimize resource allocation through information access [3]. The cloud *RAN* network makes it possible to allocate a subset of computing and caching resources, combine the necessary information and perform management functions (main signal processing, planning and allocation of radio resources, etc.). Accordingly, new cloud-based *RANs* will have greater capacity to support connectivity requirements initiated by various devices and users in globally integrated Metaverse scenarios. The need for new semiconductor components for the telecommunications market with higher bandwidth is a new serious challenge for the semiconductor industry that needs to be addressed in the medium term. Such components, such as power amplifiers, etc., significantly affect the operation of the entire system, including the output power, efficiency, throughput, etc.

Another challenge when it comes to *AI* is the availability of data using frequencies up to 330 GHz for the neural network. In the scientific literature of the field of telecommunications, special attention is paid to the research of terahertz range (THz) technologies, the purpose of which is to develop a suitable wireless system with built-in antennas in THz, where the range from 110 GHz to 170 GHz is considered one of the main prospective frequency ranges for the technologies of the future generation.

The combination of future wireless networks based on *AI* and terahertz technologies is a new research area that requires deep skills with big data, service-aware security, deeper virtualization and networks for cloud *RAN* based on international standards. The European Consortium of Academic and Industry Leaders (*Hexa-X*^[1]), which is headed by the Finnish communications company Nokia, is currently forming a policy on systematization and preliminary standardization, as well as harmonization of global standardization of innovative technologies [4]. The standardization outlines potential system designs, use cases and performance targets for new technologies that aim to enable widespread user access, high bandwidth efficiency for future heterogeneous services and applications, including virtual/augmented reality (VR/AR), holographic telepresence, Industry 4.0 and robotics. According to research by Ecorys, in Europe the VR/AR market size was estimated at €9.6 billion in 2021, up 26% from 2020, and its market value is expected to grow from 35 to 65 by 2025 billion euros [5].

[1] For reference. Hexa-X also includes the Swedish operator Ericsson and other operators.

The ISO/IEC JTC 1/SC 42 “Artificial Intelligence” Joint Technical Standardization Committee has now developed and published standards in the field of testing AI-based systems, functional safety and AI systems, big data, etc. [6].

The use of a large array of electronic data and digital technologies in the field of telecommunications and their interconnection leads to rapid changes and requires the outline of a holistic, standardized approach to the functioning of systems. In Ukraine, the creation of a new platform for the development of the technological innovation system has been launched. The Ministry of Economy initiated the pilot project “Digitization of standardization processes” regarding the involvement of AI, and the corresponding technical standardization committee was formed, the purpose of which is to ensure the standardization system in the field of AI technologies. The development of standards with the help of AI will allow speeding up the process of creating standards, reduce labor costs for development, and digitize the processes of forming standards texts. Bringing domestic standards into line with international norms and regulations with the help of AI will accelerate the selection of the optimal model of the Metaverse. The Metaverse is a future, sustainable and interconnected virtual environment of augmented reality using RAN and terahertz spectrum.

The most famous studies on the telecommunications market and related applications and services are: spectrum testing for frequencies from 95 GHz to 3 THz (US Federal Communications Commission (*FCC*)); terahertz frequency range, which provides a data transfer rate of 100 times faster than 4G (*LTE*) networks (South Korea Research Institute of Electronics and Telecommunications); development of microchips for data separation and more efficient management of terahertz waves (Universities of Osaka (Japan), Oulu (Finland) and Australian University of Adelaide); testing of integrated joint communication and sensing (*Rohde & Schwarz* company) and others.

References

1. Braten, A.E.; Kraemer, F.A.; Palma, D. Autonomous IoT Device Management Systems: Structured Review and Generalized Cognitive Model. *IEEE Internet Things J.* 2021, 8, 4275–4290.
2. Cheng, N.; Quan, W.; Shi, W.; Wu, H.; Ye, Q.; Zhou, H.; Zhuang, W.; Shen, X.; Bai, B. Space-air-ground Network Integration: A Comprehensive Simulation Platform. *IEEE Wirel. Commun.* 2020, 27, 178–185.
3. Checko, A.; Christiansen, H.L.; Yan, Y.; Scolari, L.; Kardaras, G.; Berger, M.S.; Dittmann, L. Cloud RAN for Mobile Networks-A Technology Overview. *IEEE Commun. Surv. Tutor.* 2014, 17, 405–426.
4. 6G series: Leading the way to 6G with Hexa-X II. URL: <https://www.ericsson.com/en/blog/2023/1/hexa-x-ii-leading-the-way-to-6g>
5. XR and its potential for Europe. URL: <https://glue.work/2022/10/18/xr-and-its-potential-for-europe/>
6. ISO/IEC JTC 1/SC 42 Artificial intelligence. URL: <https://www.iso.org/committee/6794475.html>

АНАЛІЗ АЛГОРИТМІВ ДИНАМІЧНОГО КЕРУВАННЯ РЕСУРСАМИ МЕРЕЖЕВИХ СЛАЙСІВ

Храбан Д.А., Скулиш М.А.

*Навчально-науковий інститут телекомунікаційних
систем, КПІ ім. Ігоря Сікорського*

E-mail: adamthebest2015@gmail.com, mskulysh@gmail.com

ANALYSIS OF ALGORITHMS FOR DYNAMIC RESOURCE MANAGEMENT OF NETWORK SLICES

In this study, we propose a reinforcement learning (RL)-based framework for dynamic resource allocation in end-to-end network slicing with heterogeneous requirements within multi-layer MEC environments. We first outline a hierarchical multi-access edge computing (MEC) architecture and formulate a resource allocation problem for end-to-end network slicing as an optimization task using the Markov decision process (MDP). Subsequently, leveraging proximal policy optimization (PPO), we develop both independently-collaborative and jointly-collaborative dynamic resource allocation algorithms to maximize resource efficiency while ensuring QoS for slices.

Швидке поширення мобільних послуг і зростання Інтернету речей та інтелектуальних пристроїв у останні роки поставили перед мережами 5G значні виклики. Цей збільшений обсяг трафіку, спричинений розвитком мобільних додатків, таких як доповнена реальність і потокове передавання 3D-відео, потребує від мереж 5G підтримки різних випадків використання, включаючи чутливі до затримки критично важливі послуги, такі як кіберфізичні системи та програми для автономного водіння. Гнучка мережева архітектура стає невід'ємною для вирішення різноманітних вимог до ресурсів та розгортання різних послуг, тому мережевий слайсінг стає ключовою технологією для задоволення цих потреб. Індивідуальне керування ресурсами у мережах доступу та базових мережах може призвести до неоптимальної продуктивності, що підкреслює важливість структури наскрізного мережевого слайсінгу, яка об'єднує ресурси на всіх рівнях.

Включення периферійних обчислень із множинним доступом (MEC) у мережі 5G наближає обчислювальні можливості до мобільних пристроїв, покращуючи показники щодо затримки, розвантажуючи робоче навантаження на найближчі сервери. Очікується, що поєднання MEC із мережевим слайсінгом оптимізує мережеві операції та надання послуг, задовольняючи різноманітні вимоги до послуг. Незважаючи на ці потенційні переваги, дослідження динамічного управління ресурсами для наскрізного мережевого слайсінгу на основі MEC у середовищах 5G все ще тільки починаються.

Навчання з підкріпленням (RL) стало цінним підходом для вирішення проблем управління мережевим слайсінгом в мережах 5G. RL дозволяє агенту побудувати оптимальну політику взаємодії з його середовищем, можливість, особливо покращена за допомогою методів глибокого навчання, таких як глибокі Q-мережі. Конкуренція за ресурси між слайсами з різноманітними характеристиками трафіку та вимогами до якості обслуговування (QoS) підкреслює

необхідність узгоджених стратегій розподілу ресурсів для підвищення продуктивності всієї мережі.

Запропонований підхід полягає у проектуванні ієрархічної архітектури для оцінки наскрізної затримки та ефективності використання ресурсів на основі характеристик слайсу. Затримка обслуговування, що включає затримку обробки та затримку передачі, розглядається як комплексний показник для оцінки наскрізної продуктивності. Для впровадження динамічного розподілу ресурсів розроблено кілька алгоритмів на основі Proximal Policy Optimization (PPO) з метою максимізації ефективності використання ресурсів, одночасно враховуючи різноманітні характеристики мережевих слайсів. Ці алгоритми працюють у рамках децентралізованого виконання, коли кожен алгоритм використовує підходи розподіленого та централізованого навчання відповідно. Оцінки продуктивності, проведені в типовому середовищі МЕС, проливають світло на неявний зв'язок між станом і дією, демонструючи ефективність запропонованих алгоритмів у покращенні ресурсоефективності та якості обслуговування.

Архітектура наскрізної системи мережевого слайсінгу будується як ієрархічна структура, що складається з кількох вузлів МЕС, кожен із яких має власні обчислювальні та комутаційні можливості. Вузли організовані в топології дерева, з шарами, позначеними як L , і вузлами МЕС, позначеними як m . Шари простягаються від основних вузлів до листових вузлів, з однаковим розміром на всіх шарах. Мережа складається з різних слайсів, позначених як n , пристосованих до різних типів трафіку користувачів і характеризується конкретними вимогами до продуктивності, такими як допустима затримка, швидкість передачі даних і робоче навантаження. Параметри, включаючи вимоги до затримки (d^n), швидкості надходження (λn) і довжини потоку (μn), визначаються для кожного слайсу, щоб кількісно визначити його показники продуктивності.

Інфраструктура мережевого слайсінгу описана з наголосом на створенні слайсів для обслуговування різноманітних типів послуг на основі вимог користувачів. Кожен слайс пов'язаний із певними показниками продуктивності, включаючи допустиму затримку та швидкість передачі даних, що визначається такими параметрами, як швидкість надходження потоку та довжина. Крім того, зрізи характеризуються щільністю обробки (ωn) і вимогами до ЦП ($w_n(t)$), причому остання розраховується на основі швидкості передачі даних і вимог до ресурсів обробки. Модель забезпечує всебічну структуру для аналізу робочого навантаження та потреб у ресурсах різних слайсів з часом, сприяючи динамічному розподілу ресурсів на основі мінливих умов мережі та вимог користувачів.

Модель системи служить основою для подальшої розробки та оцінки алгоритмів розподілу ресурсів. Визначаючи мережеву архітектуру, характеристики слайсу та показники продуктивності, модель дозволяє оцінити використання ресурсів і QoS у наскрізній інфраструктурі мережевого слайсінгу. Ця детальна характеристика мережевих компонентів і параметрів слайсів інформує про проектування та впровадження стратегій динамічного розподілу ресурсів, спрямованих на максимізацію ефективності використання ресурсів і задоволення вимог QoS для різноманітних типів послуг у багаторівневих середовищах МЕС.

Розподіл ресурсів передбачає визначення пропорції робочого навантаження та

трафіку, що проходить через вузли МЕС, на основі виділених ресурсів і оцінки робочого навантаження. Система прагне задовольнити вимоги до затримки для кожного слайсу, враховуючи затримки обробки та передачі. Порушення QoS виникають, коли затримки перевищують попередньо визначені порогові значення, підкреслюючи важливість ефективного розподілу ресурсів для задоволення різноманітних вимог до слайсів і забезпечення своєчасного надання послуг.

Основна мета полягає в оптимізації розподілу ресурсів для мінімізації затримок і максимального задоволення QoS між слайсами мережі. Замість того, щоб мінімізувати затримку, увага зосереджена на адаптивному розподілі ресурсів між рівнями МЕС, щоб збалансувати ефективність використання ресурсів і якість обслуговування. Цей підхід має на меті забезпечити ефективний розподіл робочого навантаження та своєчасне надання послуг у багаторівневих середовищах МЕС.

У сфері розподілу ресурсів для кількох слайсів мережі централізований підхід із суперагентом, здатним повністю спостерігати за станом системи та приймати рішення для всіх слайсів, може бути ідеальним з точки зору продуктивності. Однак така стратегія часто є непрактичною через великі витрати на оповіщення, які вона несе, особливо зі збільшенням кількості слайсів. Отже, децентралізовані підходи стають більш сприятливими. У роботі прийнято два децентралізовані методи, засновані на алгоритмі Proximal Policy Optimization (PPO), що пропонує більш практичне та масштабоване рішення. PPO оптимізує обрізану сурогатну цільову функцію, штрафуючи великі зміни політики та забезпечуючи стабільні оновлення політики.

Proximal Policy Optimization - це алгоритм навчання з підкріпленням, який прагне максимізувати накопичені винагороди шляхом ітеративного оновлення параметрів політики на основі спостережуваних станів і дій. Сурогатна цільова функція в PPO призначена для запобігання надмірно великих оновлень політики шляхом обрізання коефіцієнта ймовірності політики, таким чином забезпечуючи стабільні та надійні оновлення політики.

Структура розподілу ресурсів на основі PPO передбачає ітераційне оновлення параметрів політики та критичних оцінок, щоб максимізувати загальну функцію винагороди в усіх слайсах мережі. Цей підхід містить параметр відсікання для контролю величини оновлень політики, підвищуючи стабільність і надійність оптимізації політики. Збалансовуючи ефективність використання ресурсів і міркування щодо QoS, PPO пропонує надійний підхід до децентралізованого управління ресурсами в середовищах наскрізного мережевого слайсінгу. Стабільність і надійність алгоритму роблять його придатним вибором для оптимізації розподілу ресурсів, одночасно задовольняючи вимогам QoS у різних слайсах мережі.

Запропонований у роботі підхід до незалежного розподілу ресурсів на основі PPO дозволяє кожному слайсу мережі автономно оновлювати свої мережеві параметри на основі індивідуальних траєкторій. Цей метод має на меті максимізувати глобальну винагороду шляхом навчання політик мережевого агента приймати рішення щодо розподілу ресурсів незалежно для кожного слайсу, тоді як критичні мережі оцінюють функцію цінності для визначення ефективності цих рішень. Спостереження та дії кожного слайсу, включаючи таку інформацію, як тип

служби, вхідний вузол, використання ресурсів і ефективність розподілу ресурсів, використовуються у процесі прийняття рішень. Мета полягає в тому, щоб отримати оптимізовану політику, яка разом максимізує загальну винагороду в усіх слайсах.

Алгоритми передбачають послідовний збір даних протягом визначеного періоду, а потім навчання мережевих агентів для кількох епох. Протягом періоду збору даних спостереження та дії записуються, а траєкторії зберігаються в буферній пам'яті. Згодом, у період навчання, функція переваги оцінюється за допомогою узагальненого методу оцінки переваги, а обрізана сурогатна цільова функція обчислюється для оновлення мережевих агентів. Критичні значення мережі також оновлюються за допомогою функції втрат, щоб мінімізувати розбіжність між прогнозованими та фактичними значеннями.

Незважаючи на те, що в алгоритмах використовується децентралізований підхід до розподілу ресурсів у мережевому слайсінгу, виникає проблема з обмеженнями в точному оцінюванні загального впливу окремих дій слайсів на загальну винагороду. Для її вирішення запроваджується підхід спільного розподілу ресурсів на основі PPO, спрямований на покращення координації між слайсами шляхом спільного оновлення критичних мереж усіх слайсів. Цей метод спрямований на досягнення кращої оцінки глобальної функції значення стану, тим самим підвищуючи оптимізацію розподілу ресурсів між кількома слайсами для максимізації загальної винагороди.

Також вивчається якість обслуговування (QoS) за різних рівнів навантаження на мережу, оцінюючи продуктивність різних алгоритмів розподілу ресурсів. Результати показують, що зі збільшенням навантаження на мережу запропоновані алгоритми спільного розподілу ресурсів на основі PPO і незалежного спільного розподілу ресурсів на основі PPO ефективно балансують ресурси між слайсами для задоволення майбутніх потреб. Для порівняння, інші методи, такі як пропорційний розподіл (PD), демонструють нижчу продуктивність через їх стратегії реактивного розподілу ресурсів. Хоча Fixed Ratio (FR) добре працює за низьких навантажень на мережу, його ефективність зменшується зі збільшенням навантаження. Досліджено ефективність використання ресурсів за змінних навантажень мережі, виявивши, що запропоновані алгоритми досягають високого рівня використання мережевих потужностей, забезпечуючи QoS порівняно з традиційними методами. Погана продуктивність PD пояснюється її нездатністю адаптуватися до раптових змін попиту, незважаючи на виділення надлишкових ресурсів. Подібним чином підхід статичного розподілу FR призводить до низького рівня використання, особливо за сценаріїв низького попиту. Ці результати підкреслюють важливість адаптивних стратегій розподілу ресурсів, особливо в динамічних мережевих середовищах.

Крім того, робота досліджує компроміс між QoS і використанням ресурсів шляхом зміни ваги винагороди. Результати показують, що збільшення вагового коефіцієнта для QoS значно покращує задоволеність QoS, одночасно зменшуючи використання ресурсів. Цей компроміс підкреслює необхідність оптимізації ваги винагороди для досягнення балансу між якістю обслуговування та ефективністю використання ресурсів. Крім того, досліджується розподіл ресурсів відповідно до типів послуг, демонструючи, як різні служби розподіляють ресурси між мережевими рівнями. Результати підкреслюють ефективність розроблених

алгоритмів у розподілі ресурсів на основі характеристик сервісу, забезпечуючи оптимальне використання ресурсів у сценаріях наскрізного мережевого слайсінгу. Незважаючи на проблеми масштабованості, пов'язані з методами RL, запропоновані алгоритми демонструють багатообіцяючу продуктивність навіть у складних мережевих топологіях, хоча й із різною швидкістю конвергенції.

Дослідження заглиблюється в динамічний розподіл ресурсів у мережевому слайсінгу в рамках різномірних вимог у середовищах МЕС для підвищення ефективності використання ресурсів і забезпечення якості обслуговування. Формулюючи проблему як спільну багатоагентну задачу, дослідження розробляє алгоритми незалежної та спільної кооперативної оптимізації проксимальної політики з використанням підходу РРО. Результати моделювання демонструють кращу продуктивність запропонованих алгоритмів порівняно з існуючими методами, особливо підкреслюючи здатність алгоритмів досягати збалансованого розподілу ресурсів між різними типами послуг в ієрархічному середовищі МЕС. Запропонована робота має значний потенціал для вдосконалення управління мережевим слайсінгом у різних мережах, включаючи 5G і не тільки, а також у промислових мережах, вирішення проблем, пов'язаних зі збільшенням складності мережі та необхідністю підтримки гетерогенних послуг. Забезпечуючи автоматизоване й ефективне управління ресурсами, результати дослідження пропонують практичні рішення для майбутніх реалізацій мережевого слайсінгу, що є необхідним для оптимізації розподілу ресурсів і зниження витрат на управління в динамічних мережевих середовищах.

Література

1. Andronie, Mihai, et al. "Big data management algorithms in artificial Internet of Things-based fintech." *Oeconomia Copernicana* 14.3 (2023): 769-793.
2. Hussain, Fatima, et al. "Machine learning for resource management in cellular and IoT networks: Potentials, current solutions, and open challenges." *IEEE communications surveys & tutorials* 22.2 (2020): 1251-1275.
3. Goudarzi, Shidrokh, et al. "Uav-enabled mobile edge computing for resource allocation using cooperative evolutionary computation." *IEEE Transactions on Aerospace and Electronic Systems* (2023).
4. Kim, Y., H. Lim: Multi-Agent RL-Based Resource Management for End-to-End Network Slicing, *IEEE Access*, Vol. 9, 2021.
5. Liu, Xiaolan, et al. "Resource allocation with edge computing in IoT networks via machine learning." *IEEE Internet of Things Journal* 7.4 (2020): 3415-3426.
6. Lin, Zheng, et al. "Efficient parallel split learning over resource-constrained wireless edge networks." *IEEE Transactions on Mobile Computing* (2024).
7. Tang, Fengxiao, Yibo Zhou, and Nei Kato. "Deep reinforcement learning for dynamic uplink/downlink resource allocation in high mobility 5G HetNet." *IEEE Journal on selected areas in communications* 38.12 (2020): 2773-2782.
8. Xiong, Xiong, et al. "Resource allocation based on deep reinforcement learning in IoT edge computing." *IEEE Journal on Selected Areas in Communications* 38.6 (2020): 1133-1146.

ОПТИМІЗАЦІЯ У СФЕРІ ЗБЕРІГАННЯ ДАНИХ В ХМАРНИХ СЕРЕДОВИЩАХ: ПОШУК КОМПЛЕКСНОГО НАБОРУ КРИТЕРІЇВ

Карташов А.Д., Глоба Л.С.

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна
E-mail: kartashov.anton.ukr@gmail.com*

OPTIMIZATION IN CLOUD COMPUTING: SEARCHING FOR A COMPREHENSIVE SET OF CRITERIA

Finding a comprehensive set of criteria for optimizing distributed storage and data access in a multi-cloud environment.

Не зважаючи на те, що хмарні обчислення все ще знаходяться в стадії постійного розвитку, їх широке поширення дало змогу багатьом дослідникам та компаніям почати оцінювати реальні та подальші потенційні виклики, з якими стикається ця технологія [1].

Дані більше не створюються лише в локальних центрах обробки даних. Обсяг даних, які створюються у хмарі та за допомогою нових технологій - таких як Інтернет речей (IoT) та розподілені обчислення (edge computing) - продовжує зростати. Успішне управління даними потребує всебічного погляду на зберігання даних, як в локальних, так і в хмарних архітектурах.

Одним з ключових викликів, з яким стикаються користувачі хмарних обчислень, є вибір найефективніших та найбільш економічних методів зберігання та доступу до даних, уникнення залежності від постачальника. Існуючі критерії для оптимізації розподілу даних в багатьох хмарних середовищах охоплюють лише підмножину вимог користувачів. Незважаючи на попередні спроби дослідити ці критерії, постійний подальший розвиток технології хмарних обчислень вимагає всебічного переоцінювання таких підходів. [2]

На основі проведеного огляду літератури та сучасних стандартів хмарних обчислень для зберігання та доступу ми визначаємо складний набір критеріїв для зберігання даних у багатьох хмарах, який включає в себе розгляд широкого спектру факторів, які можуть впливати на розташування, управління та отримання даних у різних постачальників хмарних послуг. [3] Таблиця 1 показує комплексний набір критеріїв, які потрібно враховувати у майбутніх дослідженнях.

Розглянемо для прикладу визначення та метод розрахунку Індекса Переносу Даних (Data Portability Index).

Визначення: Індекс Переносу Даних (Data Portability Index) вимірює ступінь складності, з якою дані можуть бути безперешкодно переміщені або передані між різними хмарними середовищами або системами. Це охоплює можливість міграції, передачі та доступу до даних на різних платформах та провайдерах хмарних послуг.

Одиниці вимірювання: Зазвичай індекс представляється у числовій шкалі, де вищі значення вказують на більшу переносимість даних. Наприклад, масштаб може становити від 0 до 100.

Таблиця 1. Набір критеріїв для розподілу зберігання даних у багатьох хмарах.

№	Criteria Category	Specific Criteria	Possible Measurement Metric
1	Data Accessibility Criteria	Latency Requirements	Milliseconds (ms)
2		Redundancy and Availability	Availability Percentage (%)
3		Data Consistency	Data Consistency Index
4		Data Encryption	Encryption Strength (e.g., AES-256)
5	Cost and Resource Utilization Criteria	Cost Efficiency	Cost per GB/month (\$)
6		Resource Allocation	Resource Utilization (%)
7		Data Lifecycle Management	Percentage of Archived Data (%)
8	Data Type and Format Criteria	Data Classification	Data Classification Score
9		Data Format	Data Format Compatibility
10	Compliance and Security Criteria	Regulatory Compliance	Compliance Audit Score
11		Data Ownership	Data Ownership Policy Adherence
12		Security Protocols	Security Protocol Strength
13	Scalability and Performance	Scalability	Scalability Factor
14		Performance Metrics	Throughput (requests/second)
15	Data Migration and Interoperability Criteria	Data Portability	Data Portability Index
16		Interoperability	Interoperability Score
17	Vendor Lock-In and Vendor Criteria	Vendor Lock-In Mitigation	Lock-In Reduction Score
18		Vendor Reputation	Vendor Reputation Rating
19	Disaster Recovery and Backup	Recovery Time Objective (RTO)	Recovery Time Objective (RTO, hours)
20		Recovery Point Objective (RPO)	Recovery Point Objective (RPO, hours)
21		Data Backup Frequency	Frequency (e.g., per day, per week)
22		Backup Storage Redundancy	Redundancy Level (e.g., dual-site)
23	Monitoring and Reporting	Monitoring Tools	Tool Effectiveness (e.g., Score)
24		Reporting	Reporting Accuracy (e.g., Percentage)
25	Sustainability	Environmental Impact	Carbon Emission Reduction (%)
26		Energy Efficiency	Energy Usage (kWh)
27		Resource Sustainability	Resource Conservation Index

Вимірювання Індексу Переносу Даних включає оцінку різних факторів, які сприяють складності переміщення та доступу до даних на різних середовищах.

Запропоновані можливі способи вимірювання Індексу Переносу Даних:

1. Швидкість Передачі Даних:
 - a. Вимірювання: Швидкість, з якою дані можуть бути передані між різними платформами або провайдерами хмар.
 - b. Метрики: Mbps або GBps (Мегабіти або Гігабіти в секунду).
2. Сумісність Форматів Даних:

- a. Вимірювання: Ступінь сумісності форматів даних між вихідною та цільовою системами.
- b. Метрики: Оцінка сумісності на основі стандартизованих форматів даних.
- 3. Підтримка API:
 - a. Вимірювання: Наявність та сумісність інтерфейсів програмування додатків (API) для передачі даних.
 - b. Метрики: Оцінка сумісності API.
- 4. Інструменти Міграції Даних:
 - a. Вимірювання: Наявність та ефективність інструментів, призначених для міграції даних.
 - b. Метрики: Оцінка ефективності інструментів на основі функціональних можливостей, зручності використання та частки успішних операцій.
- 5. Обробка Метаданих:
 - a. Вимірювання: Здатність обробляти та зберігати метадані під час передачі даних.
 - b. Метрики: Оцінка збереження метаданих.
- 6. Вплив Відмови сервісу:
 - a. Вимірювання: Вплив перерв у роботі системи під час передачі даних.
 - b. Метрики: Тривалість та частота відмов.
- 7. Вартість Передачі Даних:
 - a. Вимірювання: Фінансові наслідки переміщення даних між різними середовищами.
 - b. Метрики: Вартість за ГБ/місяць за передачу даних.

Результатом Індексу Переносу Даних є загальний погляд на те, наскільки легко та ефективно дані можуть бути переміщені та доступні на різних платформах або провайдерах хмарних послуг.

Створення комплексної формули для Індексу Переносу Даних передбачає поєднання кількох факторів і надання відповідних ваг для відображення їх відносної важливості. Наведемо узагальнену формулу, яка включає ключові метрики:

$$\text{Data Portability Index (DPI)} = \sum_{i=1}^n W_i \times \left(\frac{M_i}{\text{Max}_i} \right),$$

де: n - кількість розглянутих метрик; W_i - вага, надана i -й метриці; M_i - вимірне значення i -ї метрики; Max_i - максимально досяжне значення для i -ї метрики; Таким чином, в дослідженні будуть проаналізовані і інші критерії оптимізації та дано їх визначення і методи розрахунку.

Література

1. Tomarchio, O., Calcaterra, D. & Modica, G.D. Cloud resource orchestration in the multi-cloud landscape: a systematic review of existing frameworks. *J Cloud Comp* 9, 49 (2020). <https://doi.org/10.1186/s13677-020-00194-7>.
2. Salil Bharany & Sandeep Sharma & Osamah Ibrahim Khalaf & Ghaida Muttashar Abdulsahib & Abeer S. Al Humaimeedy & Theyazn H. H. Aldhyani & Masha'el Maashi & Hasan Alkahtani, 2022. "A Systematic Survey on Energy-Efficient Techniques in Sustainable Cloud Computing," *Sustainability*, MDPI, vol. 14(10), pages 1-89, May.
3. Anton Kartashov and Larysa Globa Overview of the Approaches to Managing Distributed Storage and Access to Cloud Data//*Proceedings of International Conference on Applied Innovation in IT. Volume 11, Issue 2, pp. 19-29. (DOI:10.25673/112990).*

Секція 5. Сенсорні мережі та Інтернет речей

УДК 621.382

ЗАСТОСУВАННЯ СЕНСОРІВ СПРЯМОВАНОЇ ДІЇ В МОБІЛЬНИХ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ

Сушин І.О., Лисенко О. І., Авдєєнко Г.Л.

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна*

E-mail: rubin268@ukr.net

APPLICATION OF DIRECTIONAL ACTION SENSORS IN MOBILE WIRELESS SENSOR NETWORKS

The article describes antennas used for mobile sensor network nodes using telecommunication aerial platforms. The advantages of using directional antennas to increase the length of the communication line between the telecommunications aerial platform and the node are shown.

Сенсорні вузли є невід'ємними компонентами безпроводових сенсорних мереж, які оснащуються змінними або постійними антенами. Останні відіграють вирішальну роль у їх функціональності і бувають різних типів, розроблені відповідно до конкретних вимог, що базуються на таких факторах, як дальність зв'язку, енергоспоживання та умови навколишнього середовища. Тому можливість встановлювати антени різного типу попередньо або безпосередньо в польових умовах може змінювати кількість необхідних ресурсів наземно-повітряної мережі, НППМ, (БПЛА 1-го, 2-го рівнів, енергетичних ресурсів тощо), що дає вигоду у часі функціонування мережі, обміні/зборі інформації тощо. Перш за все їх поділяють на дві групи: спрямованої та всеспрямованої дії.

Сенсори (вузли) всеспрямованої дії у БСМ (безпроводних сенсорних мережах) є класичним варіантом пристроїв, які можуть приймати або передавати сигнал в усіх напрямках навколо них. Вони охоплюють (покривають) повне коло навколо своєї точки кріплення (згідно діаграми спрямованості антени, що використовується), що робить їх придатними для застосувань, коли події або зміни в середовищі можуть відбуватися з будь-якого напрямку, тобто область покриття має дозволяти їм передавати дані на центральний вузол або інші датчики поблизу. Споживання електроенергії є критичним фактором для сенсорних вузлів, особливо у БСМ, що працюють від одноразових або багаторазових джерел живлення.

Для вузлів всеспрямованої дії зазвичай використовують наступні розповсюджені типи антени:

1. Монопольна антена (рис. 1) [1]. Їх зазвичай використовують у вузлах через їх простоту та компактний розмір.

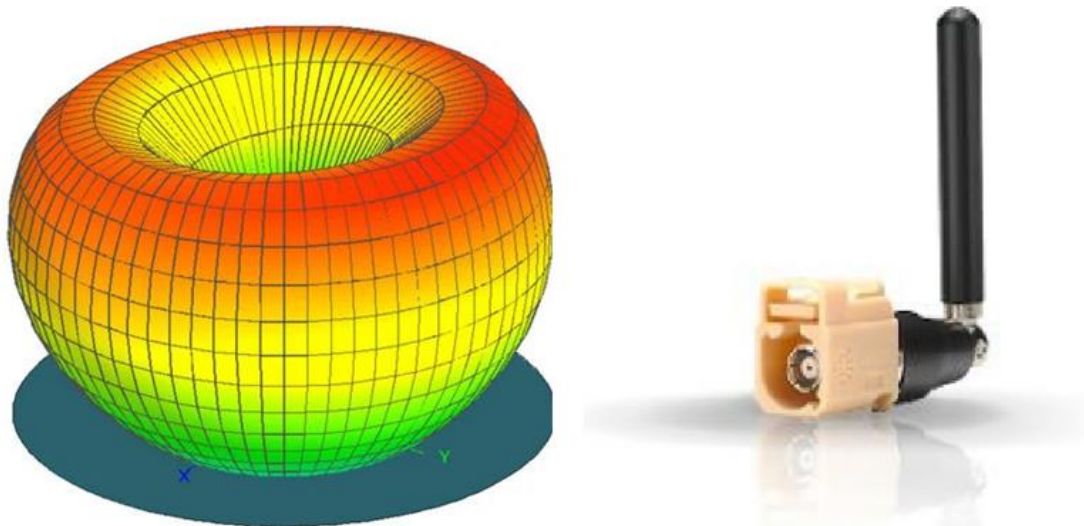


Рисунок 1. Монопольна антена та її діаграма спрямованості.

2. Дипольна антена . Це другий тип простих, але ефективних антен, які використовуються в різноманітних сценаріях, включаючи сенсорні вузли та бездротові сенсорні мережі.

3. Діско-конічна антена. Це універсальні широкопasmові антени, розраховані на вертикальну поляризацію.

Вони відносно компактні порівняно з деякими іншими широкопasmовими антенами [2]. Зазвичай мають помірне посилення, часто в діапазоні 2-5 дБі. Основною перевагою є їх широке охоплення частот, а не високе посилення.

4. Перевернуті F антени мають плоску структуру, яку можна легко інтегрувати в дизайн невеликих пристроїв. Вхідний опір даної антени залежить від відстані точки живлення від заземленого кінця. Частина антени між точкою живлення та площиною заземлення по суті поводить себе як шлейф короткого замикання. Таким чином, розробник може узгодити антену з опором лінії живлення, встановивши положення точки живлення вздовж елемента антени [3].

5. Також широко розповсюдженими є планарні антени, відомі своїм низьким профілем і придатністю для інтеграції в невеликі пристрої:

5.1. Планарна перевернута F антена (PIFA). Вона складається з плоского елемента з'єданого із короткозамкнутою або заземленою площиною.

5.2. Друкована монопольна антена — це плоска конструкція, яка часто розроблена на друкованій платі (PCB). Складається з прямого або складеного провідника з одного боку друкованої плати та заземленої площини з іншого боку.

5.3. Подібно до друкованих монопольних антен, друковані дипольні антени є планарними структурами, але мають два плеча, що простягаються в протилежних напрямках.

5.4. Планарна дискова антена — це плоска структура круглої форми, яка складається з круглого дискового елемента з заземленою площиною під ним.

5.5. Планарні щілинні антени створюються шляхом витравлювання прорізів або отворів на плоскій поверхні [4].

5.6. Мікросмугові патч-антени — це плоскі антени, які складаються з патча, надрукованого на діелектричній підкладці з заземленою площиною з іншого боку.

Маючи свої переваги, всеспрямовані датчики можуть зіткнутися з проблемами, такими як перешкоди від інших пристроїв, обмежену дію на великих відстанях і потреба в ефективних алгоритмах обробки даних для отримання даних, які передає вузол.

Спрямовані антени відіграють вирішальну роль у БСМ, фокусуючи своє випромінювання в певному напрямку, що призводить до збільшення області покриття в цільовому напрямку. Це особливо корисно для зв'язку на великі відстані, так як забезпечується більший коефіцієнт посилення порівняно з всеспрямованими антенами, що призводить до покращення потужності сигналу.

Для вузлів спрямованої дії можна використати наступні розповсюджені типи антени:

1. Антена Уда-Ягі (рис. 2). Складається з вібратора (диполя), рефлектора та одного або кількох директорів.

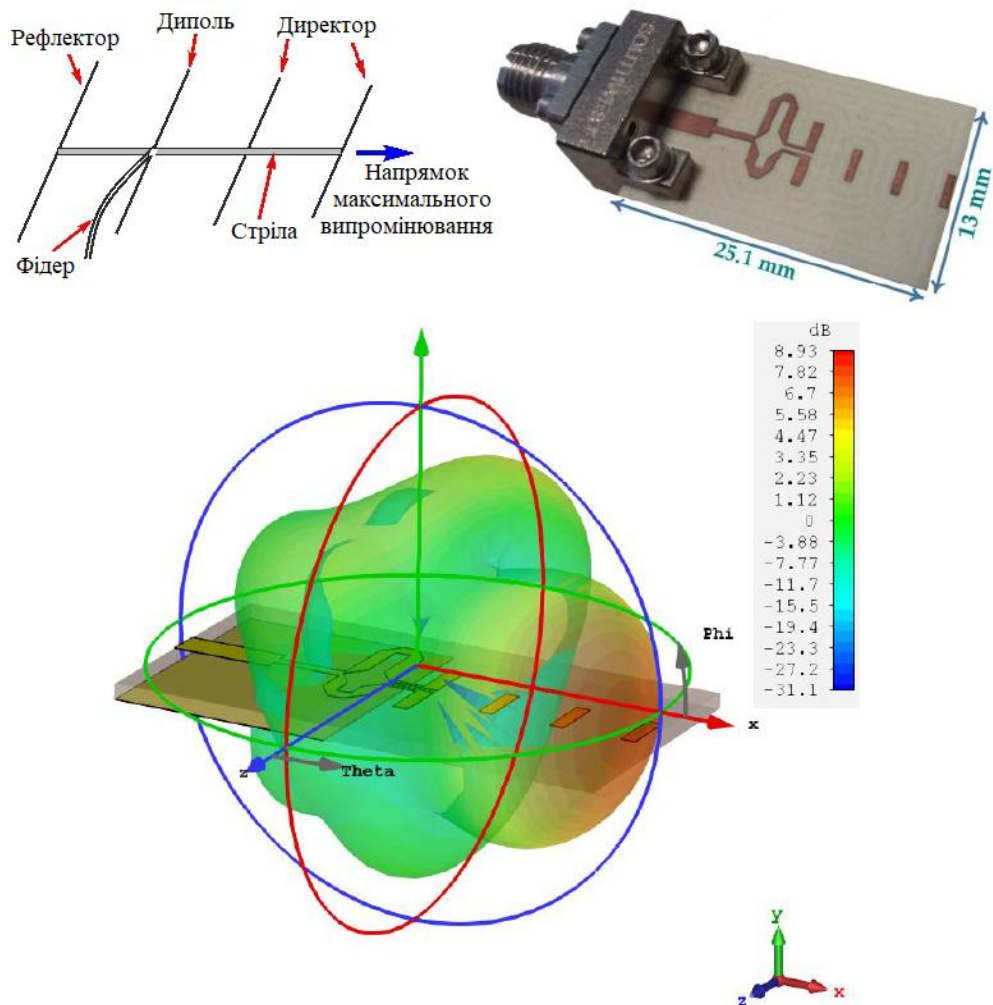


Рисунок 2. Антена Уда-Ягі та її діаграма спрямованості.

2. Параболічні антени. Можуть підтримувати різні поляризації, включаючи лінійну та кругову поляризації, залежно від конструкції елемента живлення.

3. Патч-антени. Можуть також бути побудовані для досягнення вузької діаграми спрямованості. На ширину променя патч-антени впливають її розміри.

4. Логоперіодичні антени, призначені для покриття широкого діапазону частот.

5. Антени з фазованою решіткою — це тип антенної системи, яка використовує певну кількість антенних елементів і фазообертачів для створення певних діаграм спрямованості.

6. Спиральні антени. Їх можна інтегрувати безпосередньо в друковану плату, забезпечуючи компактне та інтегроване рішення.

Основним недоліком більшості спрямованих антен є їх обмежена зона покриття, проте технологія фазованих антенних решіток дозволяє змінювати напрямок променя в залежності від потреб та сценаріїв. Розгортання та вирівнювання спрямованих антен також вимагає точності.

Таким чином, спрямовані антени є потужними інструментом, якщо необхідно встановити каналу зв'язку на великих відстанях з меншими втратами та затратами відносно всенаправлених антен. Тому проведений аналіз показує доцільність використання даного типу антен для побудови сучасних мобільних безпроводових мереж сенсорів спрямованої дії з використанням телекомунікаційних аероплатформ.

Література

1. Maxworth. A. Far-Field Radiation Characteristics of Folded Monopole Antennas over a Conducting Ground Plane. Eng 2022, 3, 142–160. <https://doi.org/10.3390/eng3010012>.
2. M. G. Tampouratzis, D. Vouyioukas and D. I. Stratakis, "Discone Rectenna Implementation for Broadband RF Energy Harvesting," 2019 8th International Conference on Modern Circuits and Systems Technologies (MOCASST), Thessaloniki, Greece, 2019, pp. 1-4, doi: 10.1109/MOCASST.2019.8741639.
3. Перевернута F-антена (IFA). Режим доступу: <https://www.electricity-magnetism.org/inverted-f-antenna-ifa/>
4. G. Q. Luo, Z. F. Hu, L. X. Dong and L. L. Sun, "Planar Slot Antenna Backed by Substrate Integrated Waveguide Cavity," in IEEE Antennas and Wireless Propagation Letters, vol. 7, pp. 236-239, 2008, doi: 10.1109/LAWP.2008.923023.

ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ КООПЕРАТИВНОГО MIMO ДЛЯ МІНІМІЗАЦІЇ ЕНЕРГОСПОЖИВАННЯ ПРИ ПЕРЕДАЧІ ДАНИХ В БЕЗДРОВОВИХ СЕНСОРНИХ МЕРЕЖАХ

Тимофєєв Є.М., Лисенко О.І.

Національний технічний університет України

“Київський політехнічний інститут імені Ігоря Сікорського”

E-mail: timofeevzh@gmail.com

APPLYING OF COOPERATIVE MIMO TECHNOLOGY TO MINIMISE POWER CONSUMPTION DURING DATA TRANSMISSION IN WIRELESS SENSOR NETWORKS

This paper explores the potential of using cooperative MIMO technology to reduce power consumption during data transmission in wireless sensor networks. The paper discusses the benefits of using cooperative MIMO technology in wireless sensor networks and how it can be used to improve energy efficiency. The authors also present a case study demonstrating cooperative MIMO technology's effectiveness in reducing power consumption during data transmission. Overall, this paper provides valuable insights into using MIMO technology in wireless sensor networks and its potential to improve energy efficiency.

Однією з основних проблем проектування бездротових сенсорних мереж (БСМ) є подолання ресурсних обмежень, що накладаються на окремі сенсорні пристрої. Одним з таких обмежень є енергоспоживання. Зі зменшенням фізичного розміру сенсорного вузла зменшується і його енергетична потужність [1]. Енергетичні обмеження в кінцевому підсумку створюють обмеження, такі як обчислювальна потужність та обмежене покриття, які призводять до архітектурних проблем.

Бездротові сенсорні мережі створюють суворі обмеження щодо енергоефективності, терміну служби мережі та надійності даних. Більшість із цих внесків знаходяться на теоретичному рівні, а також у домені бездротових сенсорних мереж не існує жодної роботи щодо ієрархічної взаємодії з віртуальним MIMO для забезпечення енергоефективності в реальних умовах WSN.

Через вимогу енергоефективності у великих мережах, концепція, відома як віртуальна MIMO, привертає все більший інтерес. У віртуальній мережі MIMO група сенсорних вузлів співпрацює для передачі та прийому даних. Ця технологія також відома як кооперативне MIMO (CMIMO). Участь декількох передавачів і приймачів у передачі дозволяє значно економити енергію при передачі даних на великі відстані [3]. Енергію можна зекономити, якщо дозволити вузлам спільно передавати дані так само, як і в режимі MIMO. Через складність схемотехніки та складність інтеграції окремих антен на сенсорних вузлах, кооперативні сенсорні вузли використовують віртуальне MIMO в бездротових сенсорних мережах для енергоефективного зв'язку та підвищення надійності даних [2].

Основними джерелами споживання енергії в сенсорних вузлах є дані зчитування, обробка даних та зв'язок. Як правило, сенсорні вузли можуть працювати в чотирьох режимах: передача, прийом, очікування та сплячий

режим. Найбільше енергоспоживання спостерігається в режимі передачі, найменше – в режимі гібернації, тоді як в режимі очікування вузли споживають енергію, яка майже дорівнює енергоспоживанню в режимі прийому.

Сформулюємо задачу ієрархічної кооперативної кластеризації МІМО як оцінку кількості кластерів, яка забезпечує мінімальне споживання енергії в мережі. Нехай $E_{заг}$ позначає загальне споживання енергії в нашій сенсорній мережі. Загальна енергія береться як сума енергії, що витрачається на внутрішньокластерний ($E_{внутр}$) та міжкластерний зв'язок ($E_{СН}$):

$$E_{заг} = E_{внутр} + E_{СН} \quad (1)$$

Вважатимемо, що сенсорні вузли рівномірно розподілені у квадратній області розміром $a \times a$. Нехай N - загальна кількість сенсорних вузлів у мережі, а k - кількість кластерів у кластерній множині K . Існує H ієрархічних рівнів.

Метою є знайти таку кількість кластерів у мережі, яка мінімізує витрати енергії для всієї множини вузлів у мережі. Цільова функція полягає в мінімізації загального споживання енергії за умови, що в мережі є k кластерів, кожен вузол належить до кластера, а відстань між головою кластера і сенсорним вузлом, що входить до нього, менша за максимальну відстань передачі вузла.

Перше обмеження забезпечує максимальний зв'язок у мережі. Друге обмеження накладає обмеження, що всі вузли бездротової сенсорної мережі повинні належати принаймні до одного кластера. Третє обмеження обмежує відстань (d) між $СН$ і сенсорним вузлом (SN), щоб вона була меншою за максимальну відстань передачі d_{tx} між вузлами. Після того, як кількість кластерів k^* знайдено, ми визначаємо кількість магістральних кластерів (RCH), які задовольняють мінімальному загальному енергетичному обмеженню в мережі, забезпечуючи при цьому $RCH \leq k$. Для повністю зв'язного графа ми прагнемо мінімізувати енерговитрати. При цьому ми переслідуюмо наступні цілі:

- збільшення терміну служби мережі;
- мінімальні витрати енергії на кожному вузлі.

Використовуючи базову енергетичну модель зв'язку для визначення кількості кластерів, ми знаходимо кількість кластерів, необхідну для мінімальних витрат енергії в мережі.

Нехай $d_{u,v}$ - середня відстань між кластерами. Очікувана відстань між кластером/вузлом u та кластером/вузлом v з координатами (x_i, y_i) та (x_j, y_j) задається [4]:

$$m[d_{u,v}] = \iint R \sqrt{x^2 + y^2} \frac{1}{2a} dx dy \quad (2)$$

де $x = x_i - x_j$, $y = y_i - y_j$, а довжина однієї сторони сітки дорівнює a .

Припустимо дистанційно-залежну модель вільного простору Фрісса для споживання енергії на один вузол. Таким чином, витрати енергії у сенсорному вузлі на передачу одного біта інформації на відстань d становлять:

$$E_{заг} = E_{схема} + \epsilon_{fs} (d_{доСН}^*)^2 \quad (3)$$

Енергія, необхідна для передачі одного біта від кластерної вершини до вузла, що співпрацює, також дорівнює рівнянню (3). Оскільки CCS знаходиться далеко від датчиків, ймовірно, споживання енергії відбувається за багатошляховою моделлю. Тому, припускаючи k кластерів і N/k вузлів у кластері, енергія на біт, що споживається в кластері, визначається за формулою [5]:

$$E_{CH} = \left(\frac{N}{k} - 1\right) E_{\text{схема}} + \frac{N}{k} E_{DA} + E_{\text{схема}} + \varepsilon_{mp}(d_{u,v}^*)^4 \quad (4)$$

Спочатку ми знаходимо кількість хопів у даній конфігурації мережі. Припустимо, що використовується рівномірний розподіл кластерів у даній мережі. Кожна сторона квадратного поля має $2a/\sqrt{k}$ кластерів, кількість переходів (h) у мережі приблизно визначається як:

$$h = \frac{k + \sqrt{k}k}{2} \quad (5)$$

Рівняння (6) дає кількість кластерів у мережі для багатошагового традиційного зв'язку SISO [5] (для мінімальних витрат енергії):

$$k^* = \frac{\sqrt{0,5855N\varepsilon_{fs}a^2}}{\varepsilon_{mp}(d_{u,v}^*)^4 - E_{\text{схема}}} \quad (6)$$

Енергія, споживана під час зв'язку МІМО (E_{MIMO}) — це сума локального споживання енергії, що виникає під час локального зв'язку між головою кластера та взаємодіючим вузлом, і енергії, спожитої під час зв'язку на далекі відстані.

$$E_{MIMO} = E_{\text{внутр}} + E_{CH} + E_{\text{longhaul}} \quad (7)$$

E_{longhaul} — це функція відстані D , яка включає енергію, необхідну для передачі даних від головного кластера до кооперативного вузла та передачі даних від кооперативного вузла до наступного кластера. Перший член у рівнянні (9) вказує на споживання енергії схеми на спільному вузлі, другий член вказує на споживання енергії передачі для локального зв'язку, а останній член вказує на споживання енергії під час зв'язку на великі відстані.

$$E_{\text{longhaul}} = 3E_{\text{схема}} + \varepsilon_{fs}(d_{\text{доCH}}^*)^2 + 3\varepsilon_{fs}(D_{u,v}^*)^4 \quad (8)$$

За допомогою методу першої похідної, щоб знайти мінімуми, ми диференціюємо рівняння (8) відносно k і отримуємо вираз для кількості головок кластера маршрутизації (k^*) для кооперативного зв'язку, що мінімізує загальну енергію:

$$k_{RCH}^* = \sqrt{\frac{0,1951k^*\varepsilon_{fs}a^2}{\varepsilon_{mp}(D_{u,v}^*)^4 - E_{\text{схема}}}} \quad (9)$$

Література

1. Hill, J.; Culler, D. A Wireless Embedded Sensor Architecture for System-Level Optimization, Available online: <http://webs.cs.berkeley.edu/papers/MICA-ARCH>.
2. Cohen, R.; Kapchits, B.; Israel, H. Topology maintenance in asynchronous sensor networks. Proceedings of the 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, San Francisco, CA, USA, 16–20 June 2008; pp. 542–550.
3. Ozgur, A.; Leveque, O.; Tse, D.N.C. Hierarchical cooperation achieves optimal capacity scaling in ad hoc networks. IEEE Trans. Inf. Theory 2007, 53, 3549–3572.
4. Pillutla, L.; Krishnamurthy, V. Joint rate and cluster optimization in cooperative MIMO sensor networks. Proceedings of the IEEE 6th Workshop on Signal Processing Advances in Wireless Communications, New York, NY, USA, 5–8 June 2005; pp. 265–269.
5. Kim, H.; Kim, S.W.; Lee, S.; Son, B. Estimation of the optimal number of cluster-heads in sensor network. In Knowledge-Based Intelligent Information and Engineering Systems; Springer: Berlin, Germany, 2005; pp. 87–94.

**ПІДВИЩЕННЯ ТОЧНОСТІ ОЦІНЮВАННЯ
ПАРАМЕТРІВ РУХУ НЕВЕЛИКИХ БЕЗПЛОТНИХ ЛІТАЛЬНИХ
АПАРАТІВ ЗА РАХУНОК ВРАХУВАННЯ ВІТРУ НА ОСНОВІ
ВИКОРИСТАННЯ ДРОБНИХ РЯДІВ ТЕЙЛОРУ**

Цуканов О.Ф., Якорнов Є.А.

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, м. Київ, Україна*

E-mail: cukanov-o@ukr.net

**IMPROVING THE ACCURACY OF ASSESSING
THE MOTION PARAMETERS OF SMALL UNMANNED
AIRCRAFT AT THE ACCOUNT OF WIND ACCOUNTING
BASED ON THE USE OF FRACTIONAL TAYLOR SERIES**

The possibility of using fractional Taylor series to estimate the movement parameters of small unmanned aerial vehicles, which are subject to strong wind effects, is considered. Some simulation results are presented, showing an increase in estimation accuracy of up to 20% compared to known methods.

Розглянуто можливість застосування дробових рядів Тейлору для оцінки параметрів руху невеликих безпілотних літальних апаратів, які схильні до сильного впливу вітру. Наведено деякі результати моделювання, що показують збільшення точності оцінювання до 20% порівняно з відомими методами.

В роботі [1] проведено аналіз досвіту застосування безпілотних літальних апаратів (БПЛА) країн членів НАТО та США, на основі якого визначений основний напрямок їх подальшого розвитку застосування при веденні мережецентричних операцій, як одних з елементів повітряної компоненти систем розвідки, зв'язку, навігації та ударних систем. Одним із завдань при створенні повітряної компоненти систем розвідки є визначення параметрів руху (ПР) невеликих БПЛА з високою точністю за наявності дестабілізуючих польотних факторів, таких як вітер (ударна хвиля при веденні бойових дій), зміна атмосферного тиску залежно від висоти польоту та інших. Тому для таких БПЛА траєкторію їхнього польоту слід розглядати як траєкторію об'єкта зі складним видом маневру і що складається з безлічі ділянок, кожна з яких необхідно описувати своєю системою диференціальних рівнянь, тобто характер його переміщення в просторі є траєкторією, на якій можна виділити ділянки з рівномірним рухом, різким маневром та ділянки з безперервним маневруванням об'єкта. Тому, для оцінки ПР БПЛА, який постійно маневрує, доцільно застосовувати адаптивний підхід з урахуванням рекурентного фільтра Калмана. Основним недоліком останнього є той факт, що у разі постійного короткочасного маневру фільтр Калмана завжди працюватиме на перехідній ділянці, а відомо, що максимальна точність оцінювання досягається саме на стаціонарній ділянці. Це означає, що алгоритми з перехідною ділянкою, як правило, рекурентні, не застосовні для оцінювання ПР постійно маневруючого БПЛА.

Розглянемо наступне завдання: не збільшуючи ступеня апроксимуючого полінома забезпечити підвищення точності оцінювання ПР БПЛА, що постійно

маневрує. Для цього розглянемо потенціальні можливості ряду П'юїзе [2] з однією змінною. Це формальний вираз виду

$$F(x) = \sum_{n=n_0}^{\infty} a_n x^{\frac{n}{m}}, \quad (1)$$

в якому число n_0 - ціле, число m - натуральне число, коефіцієнти a_n беруться з деякого кільця, причому коли $n < m$, коефіцієнти a_n повинні бути комплексними.

Ряд (1) у разі коли змінна x набуває речового значення, а значення $n_0 = 0$ може бути представлений у вигляді суми двох рядів

$$F(x) = T(x) + R(x), \quad (2)$$

де $T(x)$ - ряд Тейлора, а $R(x)$ - ряд, що складається з дробових членів. Назвемо ряд (2) дробовим рядом Тейлора. Відомий ряд Тейлора [3] у цілих похідних має вигляд

$$f(x) = f(x_0) + f'(x_0)(x-x_0) + \frac{f''(x_0)}{2!}(x-x_0)^2 + \dots + \frac{f^{(n)}(x_0)}{n!}(x-x_0)^n \quad (3)$$

або у загальному вигляді $f(x) = \sum_{k=0}^n f(x_0)^k \frac{(x-x_0)^k}{k!}$, $k = 0, 1, 2, 3, \dots$

Уявимо ряд Тейлора (3) для дробових похідних [2]. Для цього загальновідомий запис першого похідного для функцій $f(x) = x^k$, представимо як

$$f(x)' = \frac{d}{dx} f(x) = k x^{k-1}, \text{ або узагальнено } \frac{d^n}{dx^n} x^k = \frac{k!}{(k-n)!} x^{k-n}, \text{ а після заміни}$$

факторіалів гамма-функціями можна останній вираз подати у вигляді

$$\frac{d^n}{dx^n} x^k = \frac{\Gamma(k)}{\Gamma(k-n+1)} x^{k-n}. \quad (4)$$

Далі без суворого математичного обґрунтування введемо припущення: якщо існує ряд Тейлора для похідних, то такий ряд може існувати і з дробовими похідними для $n_0 = 0$, і речовими коефіцієнтами.

Тоді з урахуванням існування [2] дробових похідних такий ряд має вигляд

$$f(x_0) = \sum_{k=0}^n f(x_0)^k \frac{\Gamma(k)}{\Gamma(k-n+1)} (x-x_0)^{k-n}, \quad (5)$$

де $k=0, 0.5, 1, 1.5, 2, 2.5, \dots$

Назвемо додаткові члени введеного ряду дробовими. Зауважимо, що при використанні ряду Тейлора (5) не можна стверджувати, що він є схожим як ряд (1). Причиною цього є відсутність ортогональності членів одержаного ряду. Також зауважимо, що автори не претендують на математичну строгість використання ряду (4). Наше завдання: з'ясувати шляхом моделювання, що використання ряду Тейлора (4) при оцінюванні ПР БПЛА, яке маневрує, методом найменших квадратів (МНК) призведе лі до підвищення точності оцінювання порівняно з використанням ряду (1). Надія на цей виграш обумовлена тим, що використання ряду (4) дозволяє збільшити дискретність оцінки похідних складових траєкторії руху БПЛА.

Для початку порівняємо дробовий ряд Тейлора зі звичайним його поряд. Обмежимося також використанням ряду (5) для похідних не вище $3/2$ і залишимо поки що осторонь фізичний зміст коефіцієнтів при дробових похідних да спробуємо пояснити з математичної точки зору сутність дробової похідної.

Виходячи з вищевикладеного, проаналізуємо застосування введеного ряду Тейлора (4) з дробовими похідними стосовно задачі оцінювання ПР БПЛА. На рис. 1 показані результати апроксимації полінома третього ступеня з розподіленим шумом за нормальним законом з дисперсією помилки рівною 5 м^2 - штрих пунктирна лінія, на всьому інтервалі за МНК поліномами ступеня $1/2$ та 2 ступеня -

суцільна лінія, і за МНК поліномом ступеня $3/2$ через дробові ступеня $1/2$ - пунктирна лінія. З графіків видно, що помилка оцінювання при оцінюванні МНК поліномом (5) зменшується на 10-15%.

Аналогічно на рис 2. показаний результати апроксимації полінома третього ступеня з шумом розподіленим за нормальним законом з дисперсією помилки, що дорівнює 5 м^2 , - штрих пунктирна лінія, за методом МНК поліномом (4) - суцільна лінія, і дробовим поліномом $Y = a_0 + a_1 x^{0.5} + a_2 x^1$ - пунктирна лінія. Бачимо, що і в даному випадку застосування полінома з дрібним ступенем дозволяє підвищити точність оцінювання до 20%.

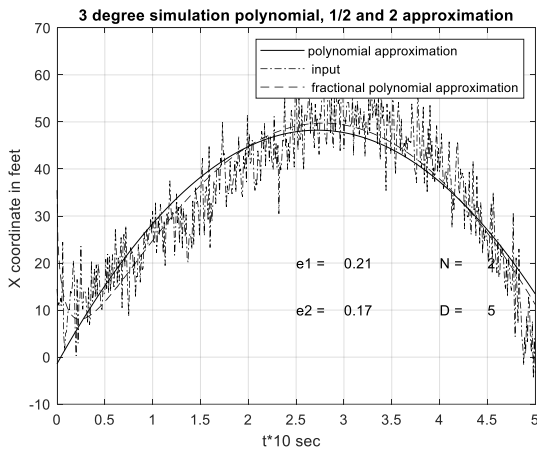


Рис. 1.

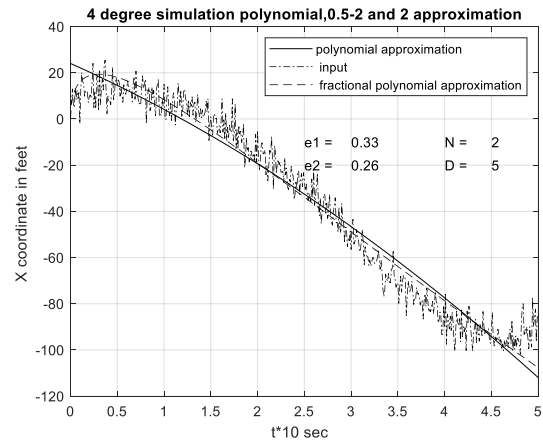


Рис. 2.

З результатів моделювання слід, що для БПЛА, яке постійно маневрує, найбільш прийнятним поліномом оцінювання є МНК з дрібними ступенями $1/2$ і, на наш погляд, необхідне подальше дослідження поліномів з дрібними ступенями вище ступеня $3/2$.

Література

1. Кучеренко Ю.Ф., Науменко М.В., Кузнецова М.Ю. Аналіз досвіду застосування безпілотних літальних апаратів та визначення напрямку їх подальшого розвитку при веденні мережецентричних операцій. Системи озброєння і військова техніка, 2018, № 1(53), с. 25-30.
2. Kilbas A., Srivastava H. and Trujillo J. Theory and Applications of Fractional Differential Equations. Amsterdam: Elsevier, 2006.
3. Sierociuk D. Fractional Kalman Filter algorithm for states, parameters and order of fractional system estimation, Int. J. Appl. Math. Comput. Sci., 2006, Vol.16, No.1, pp, 129–140.

МЕТОДИКА СИНТЕЗУ ЦИФРОВИХ РЕГУЛЯТОРІВ ПРЕЦИЗІЙНИХ ЕЛЕКТРОПРИВОДІВ ДЛЯ СИСТЕМИ ОРІЄНТАЦІЇ І СТАБІЛІЗАЦІЇ СТЕЖЕННЯ ЗА ОБ'ЄКТАМИ СЕНСОРІВ СПРЯМОВАНОЇ ДІЇ МОБІЛЬНИХ РОБОТІВ

¹Лисенко О.І., ²Фуртат С.О., ²Фуртат О.В.

¹*Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна;*

²*Таврійський національний університет імені В.І. Вернадського, Україна
E-mail: lysenko_home@ukr.net, furtatsergij@gmail.com, furtatlina@gmail.com,*

SYNTHESIS OF DIGITAL REGULATORS OF PRECISION ELECTRIC DRIVES FOR THE SYSTEM OF ORIENTATION AND STABILIZATION OF TRACKING OBJECTS OF SENSORS OF DIRECTIONAL ACTION OF MOBILE ROBOTS

The methodology recommends distinguishing two modes of operation of the electric drive: orientation (reorientation) of the sensor's sensitivity axis and its stabilization. The structure of the control law remains unchanged for both regimes. The regulation algorithm consists of digital proportional-integral-differential regulation algorithms, an algorithm for correcting the dynamic properties of the electric drive, and an algorithm for restoring (estimating) the state vector (Luenberger observer or Kalman filter). Information to the observer or filter comes from a digital ammeter. The use of the technique will allow: to improve the dynamic characteristics of the electric drive with a slight increase in energy consumption; increase reliability and reduce the load-size indicators of the electric drive.

Синтез цифрових регуляторів, які дозволяють зробити прецизійними електроприводи для системи орієнтації і стабілізації стеження за об'єктом сенсорів спрямованої дії мобільних роботів дозволять поліпшити технічні характеристики функціонування як окремих мобільних роботів, так і їх груп. Особливого значення цей факт набуває для групового застосування мобільних роботів у військових цілях. Методика синтезу цифрових регуляторів прецизійних електроприводів для системи орієнтації і стабілізації стеження за метою сенсорів спрямованої дії мобільних роботів розвиває інженерний методичний апарат синтезу цифрових регуляторів.

Суть полягає в тому, щоб завдяки алгоритмічній модернізації(удосконаленню алгоритму управління) цифрового електроприводу задовольнити дві суперечливі вимоги(критерії) : швидка переорієнтація сенсора спрямованої дії і точність його стабілізації в заданому положенні.

У методиці, що викладається, наукове завдання декомпонується на дві підзадачі: перша підзадача полягає в модернізації алгоритму переорієнтації; друга підзадача полягає в модернізації алгоритму стабілізації. Рішення першої підзадачі пропонується виконувати в детермінованій постановці, а рішення другої підзадачі - в стохастичній. При цьому міняються тільки

параметри алгоритмів управління, а їх структура залишається незмінною в результаті рішення обох підзадач. Таким чином, методика дозволяє синтезувати адаптивний до конкретного режиму роботи алгоритм цифрового автоматичного управління електроприводом системи орієнтації і стабілізації сенсора спрямованої дії.

Завдання стабілізації вісі чутливості сенсора в режимі стеження розглядається в стохастичній постановці. У цій задачі параметри обираються за умови мінімізації дисперсії помилки утримання вісі чутливості сенсора в заданому положенні та мінімізації додаткових витрат енергії автономним джерелом живлення сенсора.

Звертаємо увагу на методичні прийоми налаштування ЦСАК, які є однаковими для обох режимів її роботи. Якщо відомі параметри математичних моделей ДПС та збурення, то налаштування параметрів регулятора та спостерігача стану можна виконати заздалегідь із використанням цих моделей, тобто перед початком застосування сенсора. Якщо таких відомостей немає, то зрозуміло, потрібно виконувати оперативну ідентифікацію параметрів математичних моделей та оперативне налаштування ЦСАК під конкретну ситуацію, тобто робити ЦСАК адаптивною (квазіадаптивною).

У детермінованій постановці спостерігач стану використовує алгоритм, який носить назву спостерігач Люенбергера, а в стохастичній - фільтр Кальмана.

За результатом виконання методики отримуємо структуру математичної моделі ЦСАК у вигляді, що представлена на рисунку 1.

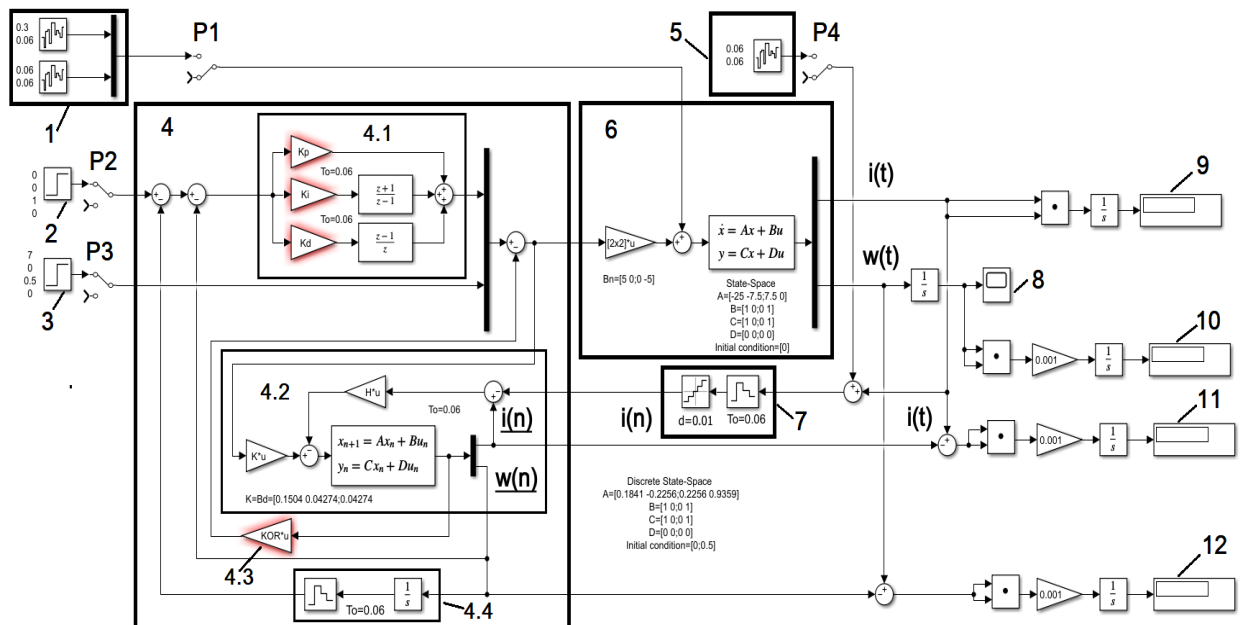


Рис.1. Структура комп'ютерної математичної моделі ЦСАК прецизійним електроприводом для системи орієнтації і стабілізації степеня за метою сенсорів спрямованої дії мобільних роботів.

Найкращим компромісним варіантом алгоритму стеження за об'єктом, що дозволяє зменшити дисперсію помилки стеження на 30% і всього в два рази збільшити споживання енергії, являється алгоритм ЦПД регулювання, використаний спільно з алгоритмом корекції динамічних характеристик електроприводу, який синтезований методом регулювання стану із бажаним(заданим) характеристичним рівнянням.

Усі алгоритми в режимі стабілізації стеження за метою використовують інформацію про вектор стану електроприводу, яка подається з виходу фільтру Кальмана.

У ЦСАК з корекцією динамічних характеристик ДПС вдається на 40% зменшити час перехідного процесу і в десятки разів зменшити амплітуду сплеску вихідного сигналу при дії ступінчастого гальмівного збурення в порівнянні з ЦСАК - без корекції динамічних характеристик ДПС.

Використання запропонованих методів дозволить: поліпшити динамічні характеристики електроприводу при незначному збільшенні витрат енергії; підвищити надійність і зменшити масогабаритні показники електроприводу. Обмеження стаціонарності математичної моделі об'єкту управління можливо замінити на квазістаціонарну, якщо в загальний алгоритм обробки інформації і управління додати алгоритм оперативної ідентифікації параметрів об'єкту управління.

Література

1. Лисенко О., Тачініна О., Алексеева І., Новіков В. Математичне моделювання руху цільового вузла Iron Bird датчиків системи керування даними безпеки. Матеріали семінару CEUR, том. 2711, стор. 482–491, (2020).
2. Lin, L., Wu, P., He, B., Chen, Y., Zheng, J., Peng, X.: The sliding mode control approach design for nonholonomic mobile robots based on non-negative piecewise predefined-time control law. *IET Control Theory & Applications*. Vol. 15(9), pp. 1286–1296. (2021). <https://doi.org/10.1049/cth2.12122>, last accessed 2023/06/10.
3. Mykhaylov, E.P., Krys, M.V.: Local navigation of mobile robots using odometry tools. *Lifting and transport equipment*. Vol. 4, pp. 21-30. (2015).
4. Mykhaylov, E.P., Skrynnyk, A.I.: Study of the means of local navigation of mobile robots. *Lifting and transport equipment*. Vol. 3, pp. 55-61. (2017).
5. Streltsov, O.V., Saftiuk, M.P.: Investigation of Methods for Interactions of a Group of Mobile Robots under Limited Communication Range Conditions. *Scientific Works of P.M. Mogilyanka Complex Chernomorsk State University. Series: Computer Technologies*. Vol. 266, Iss. 254, pp. 76-80. (2015). http://nbuv.gov.ua/UJRN/Npchduct_2015_266_254_14, last accessed 2023/06/10.
6. Alsadik, B., Karam, S.: The Simultaneous Localization and Mapping (SLAM)-An Overview. *Journal of Applied Science and Technology Trends*. Vol. 2, no. 04. pp. 120–131. (2021). <https://doi.org/10.38094/jastt204117>, last accessed 2023/06/10
7. Sebo, S., Stoll, B., Scassellati, B., Jung, M. F.: Robots in Groups and Teams. *Proceedings of the ACM on Human-Computer Interaction*, Vol. 4(CSCW2), pp. 1–36. (2020). <https://doi.org/10.1145/3415247>, last accessed 2023/06/10.

ЗАСТОСУВАННЯ ВЕЙВЛЕТ-ПЕРЕТВОРЕНЬ В ЗАДАЧАХ ОБРОБКИ СИГНАЛІВ В СЕНСОРНИХ МЕРЕЖАХ

Федорова Л.Б., Москвичова К.К.

National Technical University of Ukraine

“Igor Sikorsky Kyiv Polytechnic Institute”

E-mail: fedorova_lb@yahoo.com.ua, moskvychovakateryna@gmail.com

APPLICATION OF WAVELET TRANSFORMS IN PROBLEMS OF SIGNAL PROCESSING IN SENSOR NETWORKS

This article is devoted to the study of non-stationary signals using the mathematical apparatus of wavelet transformations, clearly demonstrates the increase in the efficiency and reliability of the functioning of sensor networks using such methods.

Сучасним методом дослідження і передачі нестационарних сигналів є математичний метод вейвлет-перетворень. Цей метод підвищує ефективність та надійність функціонування сенсорних мереж.

Для отримання максимальної величини корисної інформації з вхідного сигналу необхідні його перетворення і обробка. Більшість методів перетворення пристосовано для аналізу стаціонарних сигналів. Аналіз Фур'є встановлює поняття глобальної частоти, яка обчислюється у вигляді скалярного добутку сигналу й гармонік: $F(\omega) = \int_{-\infty}^{+\infty} f(x)e^{-i\omega x} dx$ (базовою

функцією є $\psi(t) = e^{it} = \cos t + i \sin t, i^2 = -1$). Ефективність застосування такого підходу суттєво зменшується при виникненні нестационарних компонент сигналів, так званих сплесків. Частковим вирішенням цієї проблеми є здійснення часової локалізації за допомогою віконного перетворення. Процес утворення вікна з точки зору математики – це множення функції $f(t)$ на спеціальну віконну функцію $g(t): F(\omega, t) = \int_{-\infty}^{+\infty} f(x)g(x-t)e^{-i\omega x} dx$. Віконне перетворення Фур'є пристосоване для аналізу сигналів приблизно однакового масштабу і не пристосоване для аналізу сигналів іншої структури. всі функції $g_{\omega, t}(x) = e^{i\omega x} \cdot g(x-t)$ є зсувами однієї функції зсунутої до зручного положення і заповненої високочастотними осциляціями.

Введення додаткової операції масштабування дозволяє ліквідувати ці недоліки і приводить до вейвлет-аналізу (хвилькового аналізу).

Вибираємо материнську хвильку $\psi(x)$ і утворюємо з материнської хвильки множину хвильок або аналізуючий вейвлет

$$\psi_{a,b}(x) = \frac{1}{\sqrt{a}} \psi\left(\frac{x-b}{a}\right)$$

(означає часовий зсув на b та масштабування за часом на a), що має ширину

за часом відповідну частоті ω - високочастотні є вузькими, в той час як низькочастотні є набагато ширшими. Вейвлет $\psi(x)$ повинен мати скінчену енергію: і повинен мати середнє значення рівне нулеві. Формула неперервного вейвлет-перетворення $W(a,b) = \int_{-\infty}^{+\infty} f(x)\bar{\psi}_{a,b}(x)dx$ зазвичай дискретизується і приймає вигляд послідовності аналізуючих коефіцієнтів $W_{m,n} = \int_{-\infty}^{+\infty} f(x)\psi_{m,n}(x)dx$, де $\psi_{m,k}(x) = 2^{\frac{m}{2}}\psi(2^m x + k)$.

Синтез сигналу при ортонормованому вейвлетному базисі набуває вигляду

$$f(t) = \sum_{m=-\infty}^{+\infty} \sum_{n=-\infty}^{+\infty} W_{m,n}\psi_{m,n}(t).$$

Число застосованих вейвлетів за масштабним коефіцієнтом m задає **рівень декомпозиції сигналу**. Кратномасштабний підхід, оснований на багатомасштабній здатності розрізнення, дозволяє деталізувати такий розклад

$$f(t) = \sum_{k \in \mathbb{Z}} c_k \phi_k(t) + \sum_{j=0}^{\infty} \sum_{k \in \mathbb{Z}} d_{j,k} \psi_{j,k}(t),$$

де c_k - скейлінг коефіцієнти, які зазвичай називають коефіцієнтами апроксимації сигналу і дають грубу апроксимацію сигналу, представлення, основане на низькій здатності розрізнення; $d_{j,k}$ - вейвлет коефіцієнти або коефіцієнти деталізації. На практиці значення одержаних коефіцієнтів зазвичай називають відповідно *сумами і різницями*.

Приклад вейвлетного спектрального аналізу
Розглянемо нестационарний сигнал (рис. 1).

$$x(t) = t * \sin\left(2\pi\left(t + \frac{9}{20}t^2\right)\right).$$

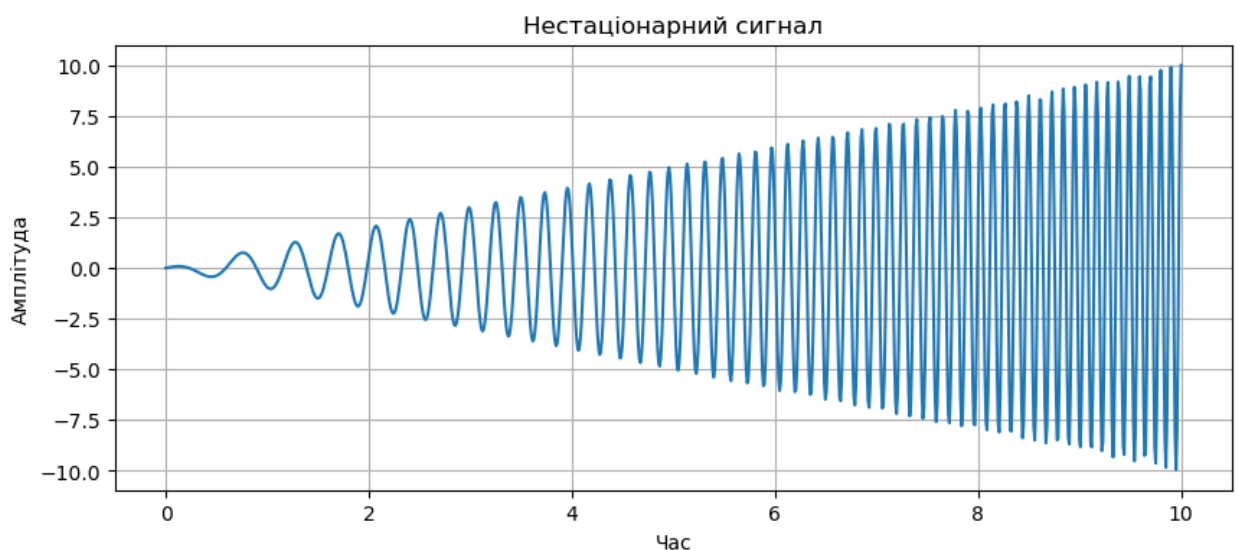


Рис.1. Нестационарний сигнал.

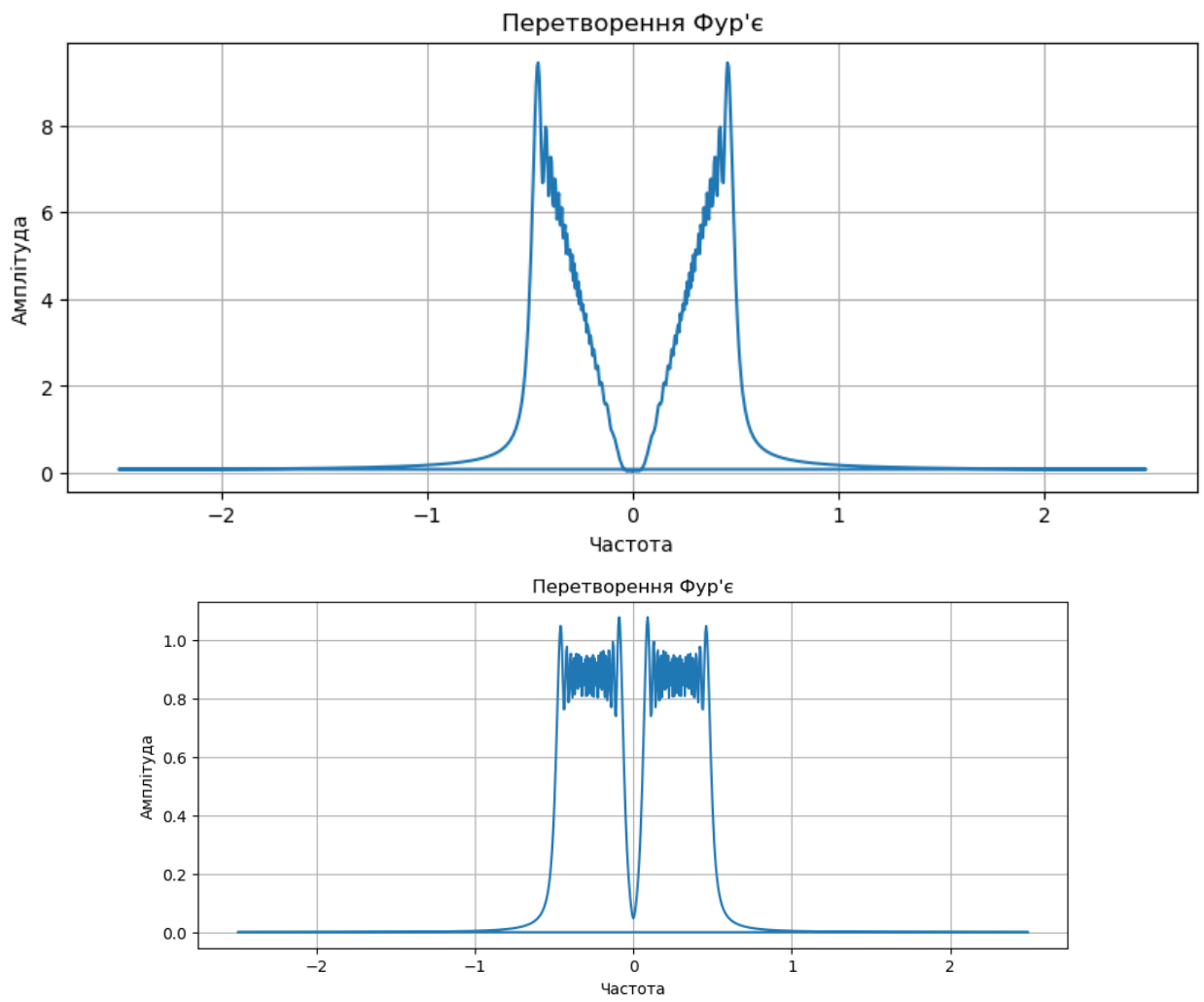


Рис.2. Перетворення Фур'є.

На оис.2 відсутня інформація про час, в який відбуваються частоти.

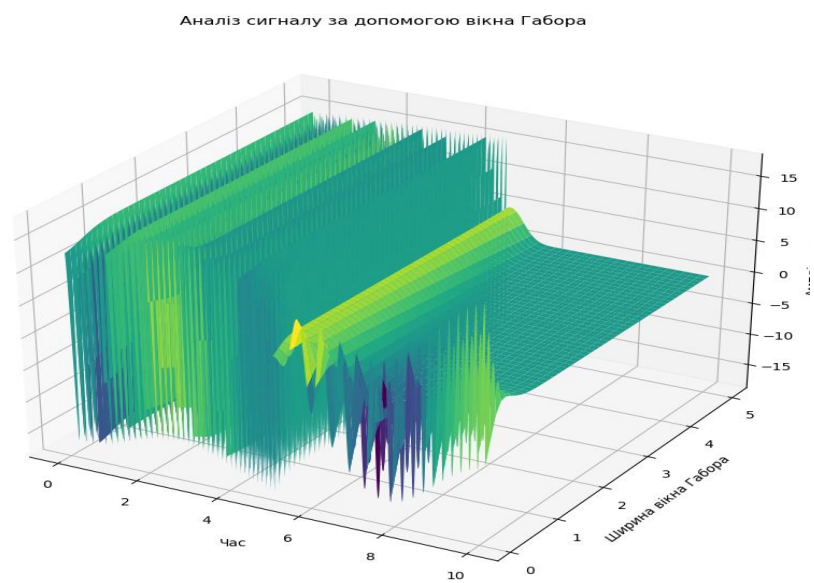


Рис.3. Вікно Габора.

З графіку рис.3 можна побачити, як амплітуда аналізованого сигналу змінюється в часі та залежить від ширини вікна.

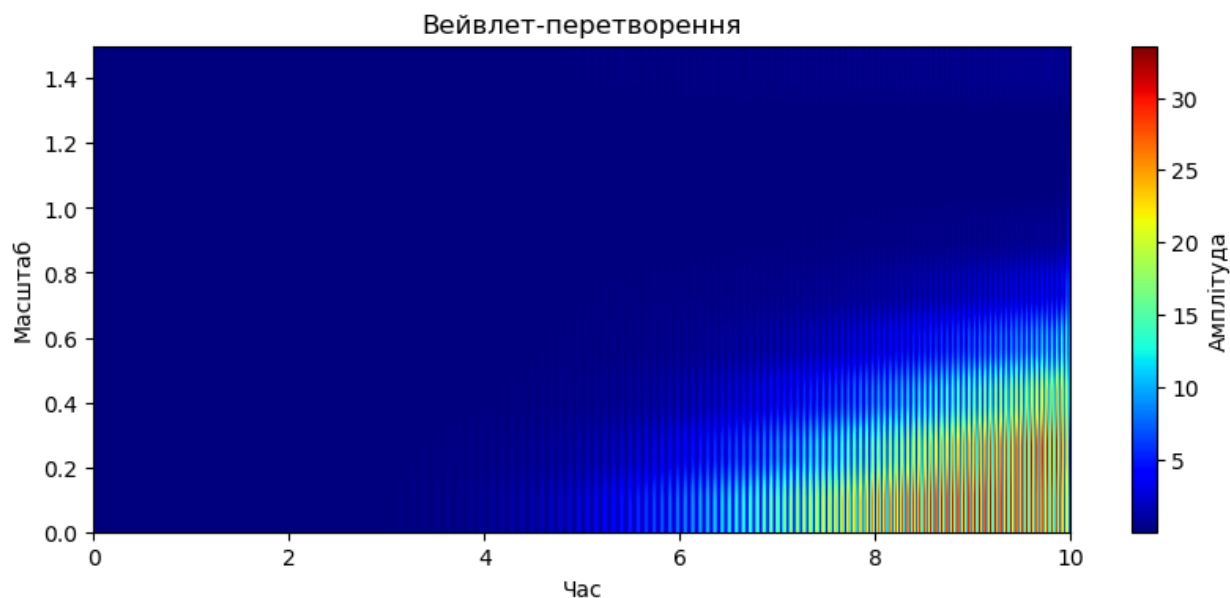


Рис.4. Вейвлет-перетворення.

Графік на рис.4 представляє результат вейвлет-перетворення сигналу, в якому використовується вейвлет Морле. Дозволяє виявити з певною точністю, коли у сигналі відбуваються зміни і на якому масштабі ці зміни виявляються найкраще.

Література

1. Геранін В.О., Писаренко Л.Д., Руцицький Я.Я. Математичні аспекти хвилькового аналізу. Навчальний посібник з 16 лекцій. Київ: ВПФ УкрІНТЕІ, 2001. – 164 с.
2. Daubechies I. Ten Lectures on Wavelets. SIAM (Society of Industrial and Applied Mathematics), Philadelphia, Pennsylvania, 1982, 357 pp.
3. Mayer Y. Wavelets. Algorithms and Applications. SIAM (Society of Industrial and Applied Mathematics), Philadelphia, Pennsylvania, Pennsylvania, 1993, 133 pp.
4. Kaiser G A Friendly Guide to Wavelets. Boston – Basel – Berlin , Birkhauser , 1994, 143 pp.
5. Robi Polikar, The Wavelet Tutorial, 2006.
6. Addison P.S. The illustration Wavelet Transform Handbook. – 2002.

АНАЛІЗ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ З ПІДТРИМКОЮ DDoS-АТАК В МЕРЕЖАХ ІoT

Аверкієв Є.О., Правило В.В.

Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна
E-mail: v.v.pravylo@ukr.net, averk1eev@gmail.com

ANALYZING MALICIOUS SOFTWARE SUPPORTING DDOS ATTACKS ON IOT NETWORKS

The scheme and purpose of DDoS attacks are considered. Three of the most dangerous malware supporting DDoS attacks on IoT networks are presented for review. General recommendations on how to effectively counteract these three malicious software are provided.

DDoS (Distributed Denial of Service) атаки використовуються для переповнення ресурсів обчислювальної техніки, роблячи її недоступною для легітимних користувачів.

Програми, що підтримують такі атаки, стали гострою проблемою через їх здатність збільшувати інтенсивність та масштаб нападів, роблячи їх більш складними для виявлення. До того ж велика кількість цих програм доступна вільно в Інтернеті та має відкритий вихідний код, що робить їх доступними для широкого кола користувачів.

Однією з популярних стратегій є використання ботнетів – мережі компрометованих пристроїв, які віддалено керуються зловмисниками. Вона може включати в себе комп'ютери, ноутбуки чи навіть підключені ІoT-пристрої.

Схема DDoS-атаки включає, переважно, одразу декілька пристроїв, що підконтрольні зловмиснику, і генерують шкідливий трафік. Як тільки атака почнеться, чистий трафік відвідувачів певного ресурсу, на який ведеться атака та шкідливий трафік зловмисника збирається в одне ціле, і йде відправка величезної кількості запитів на обчислювальну техніку, яка в результаті при відсутності додаткового захисту, повністю стає ускладненою для доступу, або ж взагалі недоступною (рис. 1).

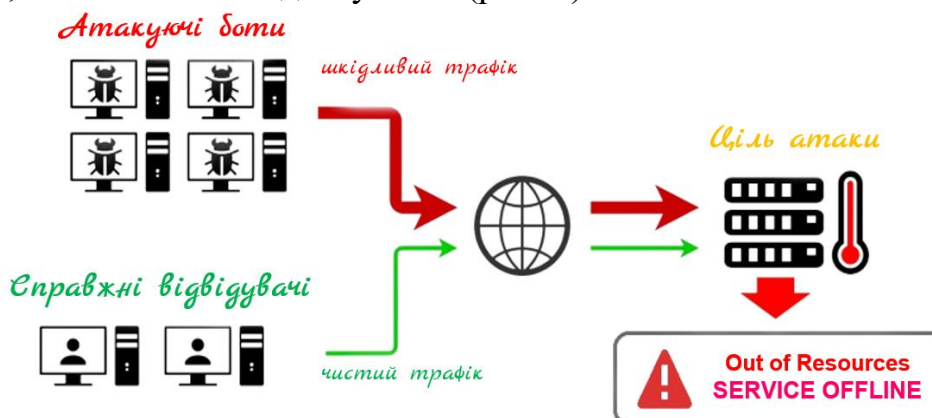


Рис.1. Схема основної роботи DDoS-атаки на ресурси будь-якого типу.

Враховуючи вищенаведену інформацію, стає зрозумілим, що DDoS-атаки становлять серйозну загрозу для цифрового світу. Вони можуть призвести до значних втрат даних, перерв у роботі служб та фінансових збитків. Особливо небезпечними є атаки на Інтернет речей (IoT), оскільки багато IoT-пристроїв не мають достатнього захисту і можуть бути легко скомпрометовані.

Вірусів, що підтримують такі DDoS-атаки існує досить велика кількість. Це пов'язано з тим, що багато з тих вірусів, що були створені на самому початку, мали відкритий вихідний код. Саме цей фактор і дозволяє зловмисникам створювати власні модифікації цих вірусів, тим самим значно збільшуючи їх загальну кількість. В рамках дослідження буде розглянуто 3 найнебезпечніших програмних забезпечення з підтримкою DDoS-атак на мережі IoT, які існують на теперішній час, а також наведено загальні рекомендації щодо їх протидії (Mirai, XOR.DDoS, Linux.Hydra).

1. Mirai:

Це шкідливе програмне забезпечення, яке стало відоме своєю здатністю зламувати та заражати пристрої Інтернету речей (IoT). Його основна мета – створення ботнету для здійснення DDoS-атак на різноманітні цілі.

Головною метою Mirai є використання заражених IoT-пристроїв для проведення DDoS-атак. Це досягається шляхом скоординованого надсилання великої кількості запитів до цільового сервера або мережі, зумовлюючи їх перевантаження та відмову в обслуговуванні. Внаслідок цього, цільовий об'єкт може перестати відповідати на легітимні запити користувачів.

Mirai також вирізняється тим, що він може самостійно розпізнавати та уникати деяких захисних заходів, що може ускладнити виявлення та подолання цього шкідливого ПЗ.

Таким чином, для забезпечення безпеки IoT-пристроїв та захисту від Mirai рекомендації можуть бути наступними:

- Встановіть сильні паролі, які складаються з комбінації великих і малих літер, цифр і спеціальних символів.
- Оновіть вбудоване програмне забезпечення (Firmware) на IoT-пристроях, включаючи оновлення безпеки.
- Налаштуйте фільтри трафіку на мережевих пристроях для виявлення та блокування аномального або потенційно шкідливого трафіку.
- Закрийте порт TCP 23 (бо саме через цей порт працюють основні компоненти ПЗ Mirai) і окремо службу Telnet на маршрутизаторі.

2. XOR.DDoS:

XOR DDoS - це троянський вірус для Linux з можливостями rootkit, який використовувався для запуску масштабних DDoS-атак. Його назва походить від інтенсивного використання XOR-шифрування як у вірусі, так і в мережевому спілкуванні з C&C. Він створений для різних архітектур Linux, таких як ARM, x86 та x64. XOR.DDoS був виявлений у вересні 2014 року групою дослідників MalwareMustDie.

XOR.DDoS використовує механізми уникнення, які дозволяють його операціям залишатися непомітними. Його можливості уникнення включають

замаскування дій вірусу, уникнення механізмів виявлення на основі правил та пошуку чужих шкідливих файлів на основі хешу, щоб прибрати «конкуренцію».

Також XOR.DDoS приховує шкідливі дії від спеціального аналізу, перезаписуючи чутливі файли нульовим байтом. Він також включає різні механізми для підтримки різних дистрибутивів Linux.

Таким чином, для забезпечення безпеки IoT-пристроїв від XOR.DDoS наступні рекомендації можуть бути впровадженими:

- Змініть паролі за замовчуванням на сильні.
- Обмежте кількість IP-адрес, з якими ваш пристрій IoT з'єднується.
- Використовуйте мережевий брандмауер та фільтрацію DNS для блокування потенційних SYN-пакетів.
- Встановить оновлення програмного забезпечення.

3. Linux.Hydra:

Linux.Hydra - інструмент для взлому паролів, який підтримує численні протоколи для атаки. Hydra працює, використовуючи різні підходи для виконання атак грубої сили, щоб вгадати правильну комбінацію імені користувача та пароля. Цей інструмент наглядно показує, наскільки легко можна було б отримати несанкціонований доступ до системи віддалено. Hydra може виконувати швидкі атаки перебором за словником проти більш ніж 50 протоколів, включаючи telnet, FTP, HTTP, HTTPS, SMB.

Для забезпечення безпеки IoT-пристроїв від шкідливого ПЗ Linux.Hydra, рекомендації можуть виглядати таким чином:

- Змініть паролі за замовчуванням на сильні.
- Налаштуйте систему, щоб вона блокувала спроби вводу паролів після N-ої невдалої кількості спроб.

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/Zhurakovskiy_B_Zeniv_Tehnologii_internet_rechey.pdf
2. Peng, T., Leckie, C., & Ramamohanarao, K. (2007). Survey of network-based defense mechanisms countering the DoS and DDoS problems. *ACM Computing Surveys*, 39(1), Article 3.
3. Granjal, J., Monteiro, E., & Sa Silva, J. (2015). Security for the internet of things: a survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials*, 17(3), 1294–1312.
4. Koliass, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: mirai and other botnets. *IEEE Computer*, 50(7), 80–84.
5. Houle, K. J., & Weaver, G. M. (2001). Trends in denial of service attack technology. Tech. Rep., CERT Coordination Center, Pittsburgh, Pa, USA.
6. Bertino, E., Choo, K.-K. R., Georgakopolous, D., & Nepal, S. (2016). Internet of things (IoT): smart and secure service delivery. *ACM Transactions on Internet Technology (TOIT)*, 16(4), Article 22.

ПАРАМЕТРИ ДЛЯ ПОРІВНЯННЯ ТРАДИЦІЙНИХ ПРОТОКОЛІВ КЛАСТЕРИЗАЦІЇ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ

Насвіт Ю.О., Лисенко О.І., Новіков В.І.

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна
E-mail: nasvit17@gmail.com*

PARAMETERS FOR COMPARING TRADITIONAL WIRELESS SENSOR NETWORK CLUSTERING PROTOCOLS

Traditional wireless sensor network clustering protocols. In this category of protocols, clustering is performed using probabilistic methods, and it does not consider any special approaches or optimization techniques for cluster formation, CH selection and data transmission. The traditional category of protocols considers the classical clustering methodology and uses basic clustering approaches for CH selection and cluster formation.



Рис.1. Традиційні протоколи кластеризації
безпроводових сенсорних мереж.

Традиційні протоколи кластеризації безпроводових сенсорних мереж (рис. 1) порівнюються на основі їх методології, функцій та продуктивності.

Параметр на основі методології розглядає параметри кластеризації, що використовуються для реалізації підходів до кластеризації. Параметр, заснований на особливостях, враховує цілі, можливості та недоліки протоколів. Параметри на основі продуктивності враховують результати моделювання різних протоколів кластеризації. На рис. 2 показано параметри порівняння на основі методології для традиційних протоколів кластеризації.

Розглядаються параметри, які використовуються для реалізації різних традиційних протоколів кластеризації. Діяльність, пов'язана з процесом кластеризації, включена з метою порівняння до параметрів, що базуються на методології. Параметри порівняння на основі методології, що використовуються для традиційних: протоколів, наведені нижче.

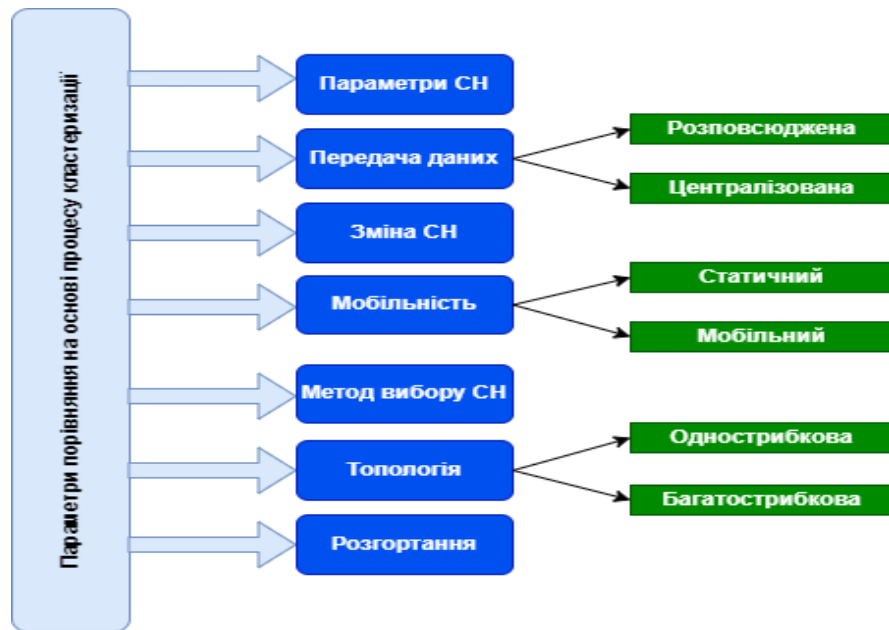


Рис.2. Параметри порівняння на основі процесу кластеризації [1].

Параметри вибору Cluster Head. Параметри вибору СН використовуються для призначення ЦТ в підходах до кластеризації для управління діяльністю кластера. Такі параметри, як енергія, сусіди, відстань до БС тощо, використовуються кластерними підходами для призначення найефективнішого вузла в якості СН. Параметри, що використовуються в процесі вибору СН, відіграють вирішальну роль у виборі відповідного вузла в якості СН серед різних вузлів, що допомагає покращити продуктивність мережі [2], [3].

Міжкластерний зв'язок. Його можна розглядати як зв'язок між СН та БС. Центральна станція може з'єднуватися з Базовими Станціями або безпосередньо, або за допомогою проміжних вузлів ретрансляції. Зв'язок може бути однострибковим або багатострибковим [4], [5]. Вузли, які знаходяться ближче до БС, використовують однострибковий зв'язок. Якщо потужність сигналу у вузлах обмежена або кількість вузлів велика, використовується політика багатострибкового зв'язку.

Внутрішньокластерний зв'язок. Його можна розглядати як зв'язок між вузлами всередині кластера. Вузли в кластері можуть дотримуватися політики однострибкового або багатострибкового зв'язку [5]. Коли розмір кластера невеликий, вузли, як правило, дотримуються однострибкового з'єднання з БС. У кластерах, де БС знаходиться далеко від вузлів, а вузли мають обмежений рівень сигналу, перевага надається багатострибковому зв'язку.

Зміна СН. Цей параметр показує, чи відбувається зміна відповідальності центральної станції змінюється між вузлами в різних протоколах кластеризації. Деякі підходи до кластеризації передбачають періодичну

заміну СН після кожного раунду зв'язку. У деяких методах СН змінюється, коли досягає певного енергетичного рівня або коли виконується певна умова. Зміна СН допомагає збалансувати енергетичні витрати вузлів [6]. Через додаткові обов'язки СН споживає більше енергії, ніж звичайні вузли, тому зміна роботи СН між вузлами допомагає уникнути раннього виведення з ладу вузла і зберігає енергію вузлів для наступних раундів.

Мобільність. Вузли, що використовуються в підходах кластеризації, можуть бути як статичними, так і мобільними. Вибір вузлів залежить від типу програми. Статичні вузли є фіксованими і не можуть змінювати своє положення [7]. Мобільні вузли є рухомими і можуть змінювати своє розташування в мережі. Статичні вузли утворюють фіксований кластер, і такими кластерами легше керувати. Кластер, сформований за допомогою мобільних вузлів, динамічно змінюється і спричиняє часту зміну топології, що вимагає регулярного обслуговування.

Метод вибору СН. Описується метод вибору СН, який використовується в різних підходах до кластеризації для призначення СН. Вибір СН має прямий вплив на загальну продуктивність мережі, оскільки більшість важливих завдань у процесі кластеризації виконує саме СН. Процес вибору СН може ґрунтуватися на ймовірнісних моделях або може бути виконаний за допомогою деяких механізмів, які враховують різні критерії вибору [7]. Цей параметр може допомогти досліднику отримати швидке розуміння процесу відбору СН, що використовується в різних традиційних протоколах кластеризації.

Топологія. Топологія мережі в протоколах кластеризації може бути розподіленою, централізованою та гібридною (комбінація централізованої та розподіленої). При розподіленій кластеризації мережа самоорганізується вузлами і кластеризація виконується вузлами без будь-якого центрального управління. При централізованій кластеризації завдання кластеризації, призначення СН, передача даних і т.д. контролюються центральним органом (базовою станцією). Гібридна топологія використовує поєднання централізованої та розподіленої топології для виконання різних завдань кластеризації [8]. Цей параметр показує тип топології, прийнятий різними протоколами кластеризації.

Політика розгортання. Вузли в робочій зоні можна розгортати, дотримуючись політики випадкового або ручного розгортання. При випадковому розгортанні вузли розміщуються випадковим чином у мережевому просторі без будь-яких попередньо визначених методів розгортання. Випадковому розгортанню надається перевага в додатках, де участь людини неможлива, і в таких випадках вузли можуть бути скинуті з

повітря і розміщені випадковим чином. При ручному розгортанні вузли розміщуються в мережі за допомогою певних методів розгортання. При ручному розгортанні вузли слідує зазначеним шляхом для маршрутизації при підключенні вузлів. Політика розгортання в кластерних підходах враховує покриття і підключення вузлів при розміщенні вузлів в зоні зондування, що впливає на тривалість роботи мережі.

Таким чином в доповіді були розглянуті параметри, які використовуються для реалізації різних традиційних протоколів кластеризації безпроводових сенсорних мереж. Розглянуті параметри кластеризації, які застосовуються для традиційних протоколів кластеризації безпроводових сенсорних мереж, не в повній мірі підходять для їх використання у безпроводових сенсорних мережах із самоорганізацією для моніторингу параметрів навколишнього середовища. Тому в подальшому пропонується удосконалення існуючих параметрів кластеризації для їх використання у протоколах кластеризації безпроводових сенсорних мереж із самоорганізацією для моніторингу параметрів навколишнього середовища.

Література

1. Rawat, P., & Chauhan, S. (2021). A survey on clustering protocols in wireless sensor network: taxonomy, comparison, and future scope. *Journal of Ambient Intelligence and Humanized Computing*. doi:10.1007/s12652-021-03381-9
2. Yadav S, Yadav RS (2016) A review on energy efficient protocols in wireless sensor networks. *Wirel Netw* 22:335–350. <https://doi.org/10.1007/s11276-015-1025-x>
3. Yahiaoui S, Omar M, Bouabdallah A et al (2018) An energy efficient and QoS aware routing protocol for wireless sensor and actuator networks. *AEU Int J Electron Commun* 83:193–203. <https://doi.org/10.1016/j.aeue.2017.08.045>
4. Taheri H, Neamatollahi P, Younis OM et al (2012) An energy-aware distributed clustering protocol in wireless sensor networks using fuzzy logic. *Ad Hoc Netw* 10:1469–1481. <https://doi.org/10.1016/j.adhoc.2012.04.004>
5. Gherbi C, Aliouat Z, Benmohammed M (2017) A survey on clustering routing protocols in wireless sensor networks. *Sens Rev* 37:12–25
6. Bayrakli S, Erdogan SZ (2012) Genetic algorithm based energy efficient clusters (GABEEC) in wireless sensor networks. *Procedia Comput Sci* 10:247–254; Pradhan S, Sharma K (2016) Cluster head rotation in wireless sensor network: a simplified approach. *Int J Sens Appl Control Syst* 4:1–10; Rostami AS, Badkoobe M, Mohanna F et al (2018) Survey on clustering in heterogeneous and homogeneous wireless sensor networks. Springer, New York; Fanian F, Kuchaki Rafsanjani M (2019) Cluster-based routing protocols in wireless sensor networks: a survey based on methodology. *J Netw Comput Appl* 142:111–142.
7. Rajendra Prasad D, Kiran Kumar B, Indraneel S (2020) Mobility in wireless sensor networks. In: *Lecture notes on data engineering and communications technologies*. Springer, pp 165–171.
8. Lei Y, Shang F, Long Z, Ren Y (2008) An energy efficient multipleshop routing protocol for wireless sensor networks. In: *2008 first international conference on intelligent networks and intelligent systems*. IEEE, pp 147–150; Yueyun C, Yue-Long Z, Jianwei A, Qian L (2012) An energy-saving routing protocol based on LEACH. In: *2012 fourth international conference on multimedia information networking and security*. IEEE, pp 608–611.

ВИКОРИСТАННЯ КОНЦЕПЦІЇ РОЗПОДІЛЕНОГО СУПУТНИКА ДЛЯ ПОБУДОВИ КОСМІЧНОГО СЕГМЕНТУ СИСТЕМИ STARLINK

Явісія В.С., Лисенко О.І.

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна
E-mail: yavisya42@gmail.com*

USING THE CONCEPT OF DISTRIBUTED SATELLITE FOR BUILDING THE SPACE SEGMENT OF THE STARLINK SYSTEM

The architecture of the Starlink system ensures the presence in orbit of tens of thousands of expensive satellites, which fail quite often. At the same time, all satellite equipment is lost, even if it is working. To reduce such losses, it is suggested to use the approach of a distributed structure of society.

Останніми роками відбувається справжня космічно-технологічна революція під назвою Starlink. До недавнього на навколоземній орбіті не було жодного супутника системи, але на сьогодні це одна з найбільших систем супутникового зв'язку (ССЗ). Попри те, що системі ще дуже далеко до завершення розгортання, вона вже функціонує та поступово змінює наш світ, зокрема допомагаючи Україні протистояти повномасштабному російському вторгненню [1].

Наразі архітектура системи Starlink складається з трьох основних компонентів: угруповання супутників на низьких орбітах, мережі наземних станцій, а також терміналів користувачів.

Абсолютна більшість супутників Starlink розміщена на орбітах висотою 540-550 км, що значно зменшує затримку сигналу до кінцевого споживача. Другий етап розвитку системи передбачає створення ще одного сузір'я з 7518 апаратів, які будуть розміщені на орбітах висотою 330-350 км. Ці супутники працюватимуть у V-діапазоні [1].

У перспективі компанія SpaceX планує збільшити кількість активних супутників до 42 тисяч. Це величезна цифра. Але, враховуючи успіхи SpaceX у здешевленні вартості запусків та серійного виробництва апаратів, вона вже не виглядає такою неймовірною, як лише кілька років тому.

Супутники Starlink, як і всі інші штучні супутники, піддаються постійному впливу різноманітних факторів, які пришвидшують їх деорбітацію. Так, наприклад, ще в лютому 2022 року 40 супутників Starlink пошкодила потужна геомагнітна буря.

Станом на березень 2024 року, Starlink вже запустила 5240 супутників, але в робочому стані перебувають не всі апарати. На сьогодні понад 570 супутників було знищено сонячними бурями та іншими проблемами [2].

Відмова апарату може відбутись через несправність або некоректну роботу лише одного елемента певної системи. Це призводить до втрати

решти іншого, а головне, справного обладнання, що розташовано на супутнику. З погляду на таку сумну статистику відмов, пропонується використати концепцію розподіленого супутника, згідно якої функціональні блоки кожної системи будуть знаходитись в фізично окремому корпусі [3]. Тоді великий супутник Starlink можна замінити угрупованням (кластером), що, наприклад, складається з декількох малих наносупутників (НС) формату CubeSat. Необхідна кількість НС обчислюється сотнями тисяч, тому промислове виробництво такої кількості апаратів може бути суттєво здешевлено і призведе до зменшення вартості космічного сегменту.

Склад кластеру із НС може бути не однорідним з погляду на функції, що виконуються окремими апаратами: основна частина НС може використовуватися для зв'язку із абонентськими терміналами, інші – для концентрації і комутації навантаження всередині кластеру, зв'язку із сусідніми кластерами НС, які розташовані на власній та суміжних орбітах, а також для зв'язку із наземними станціями. Оскільки відстань між НС кластеру складає лише кілька десятків метрів, взаємодія між ними може здійснюватися за допомогою *Wi-Fi* або лазерного променя [4]. Склад кластеру пояснює рис.1.

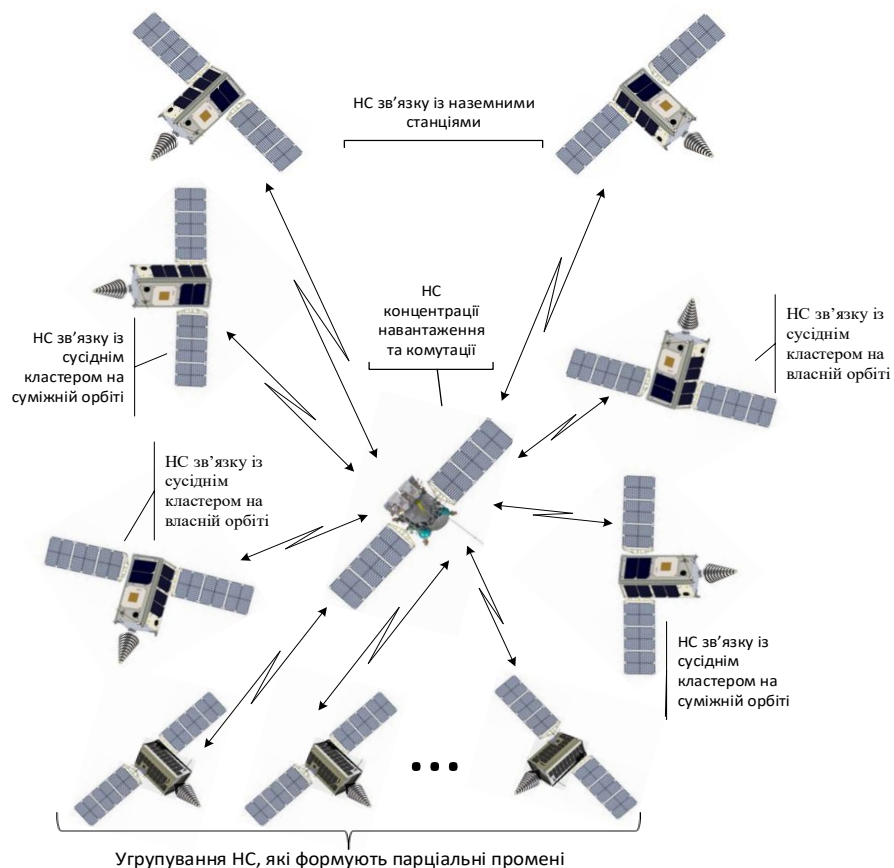


Рис.1. Склад кластеру із НС.

Приблизний склад НС угруповання може визначатися наступним чином. Найбільша кількість НС буде призначена для зв'язку із абонентськими терміналами, НС даної категорії необхідні для формування

парціальних променів, з яких утворюється певна зона покриття. Функцію концентрації і комутації навантаження всередині кластеру може виконувати один НС (бажано із дублюванням). Для зв'язку із іншими кластерами на власній та суміжних орбітах – чотири НС, для зв'язку із наземними станціями – два НС [5].

При такому підході втрата окремого НС не призведе до відмови всього кластеру, скоріш за все відбудеться незначне погіршення окремих показників (зменшення пропускнуої спроможності або зменшення кількості терміналів, які обслуговуються), тоді як при використанні великих супутників можлива повна втрата функціоналу, який виконує такий апарат. Оскільки функціонування ССЗ Starlink передбачає періодичний запуск на орбіту нових носіїв з супутниками для оновлення угруповання, згодом втрачений НС можна замінити новим і таким чином відновити функціонал кластеру.

За рахунок використання розподіленого супутника ефективність супутникового сегменту на базі НС виявляється значно вищою у порівнянні із існуючими ССЗ. Окрім того, запропоноване рішення в цілому підвищує надійність усієї системи, оскільки втрата або вихід з ладу окремих НС незначним чином вплине на характеристики угруповання, а у випадку часткового резервування НС в кластері такі події можуть бути повністю нівельовані [6]. Немаловажним є і той факт, що з'являється можливість поетапного оновлення космічного сегменту. Використання НС вирішить проблему космічного сміття, оскільки НС будуть знаходитись на низькій орбіті та по закінченні своєї місії будуть повністю згорати в земній атмосфері.

Література

1. Starlink. Як влаштована система глобального супутникового інтернету. <https://universemagazine.com/starlink-yak-vlashtovana-systema-globalnogo-suputnykovogo-internetu>.
2. Starlink. https://uk.wikipedia.org/wiki/Starlink#cite_note-178.
3. Низькоорбітальна супутникова система інтернету речей на базі розподіленого супутника / Ільченко, М.Ю., Наритник, Т.М., Присяжний, В.І., Капштик, С.В., Матвієнко, С.А. / Космічна наука і технології. 2020, №4 (125): с.57-85 / <https://doi.org/10.15407/knit2020.04.057>.
4. Monitoring System and Fixed Communication on the Basis of Nanosatellites. Lysenko, A., Yavisya, V., Alekseeva, I., Tureichuk, A. 2018 International Scientific-Practical Conference on Problems of Infocommunications Science and Technology, PIC S and T 2018 - Proceedings, 2019, pp. 495–498, 8632097.
5. Approach to building a national satellite communications system. Sparavalo, M., Yavisya, V., Lysenko, A., Tureichuk, A. 2019 International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019 - Proceedings, 2019, 9165399.
6. Concept of Construction of Satellite Communication and Navigation System clear Space. Tachinina, O.M., Lysenko, O.I., Yavisya, V.S., Alekseeva, I.V. 2020 IEEE 6th International Conference on Methods and Systems of Navigation and Motion Control, MSNMC 2020 - Proceedings, 2020, pp. 110–113, 9255538.

МЕТОДИ ЕЛЕКТРОЖИВЛЕННЯ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ

Явісія В.С., Лисенко О.І.

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна
E-mail: yavisya42@gmail.com*

METHODS OF POWERING WIRELESS SENSOR NETWORKS

The main aspects of the energy consumption of a wireless sensor network are considered. To increase the lifetime of both individual sensors and the wireless sensor network as a whole, it is proposed to implement a strategy of dynamic power management of the main sensor subsystems.

Ефективність функціонування безпроводової сенсорної мережі (БСМ) визначається багатьма факторами [1]. Значний вплив на збільшення тривалості надійної роботи БСМ здійснюється за рахунок обґрунтованого вирішення задачі керування трафіком [2] та обрання енергоефективних способів електроживлення.

Енергоспоживання БСМ є надзвичайно важливим через дефіцит енергії. Хоча енергія є дефіцитним ресурсом у кожному безпроводовому пристрої, проблема в БСМ посилюється з наступних причин:

1. Порівняно зі складністю завдання, яку вони виконують, а саме, зондування, обробка, самокерування та зв'язок, вузли мають дуже малий розмір для розміщення джерел живлення великої потужності.

2. В ідеалі, БСМ складається з великої кількості вузлів. Це робить ручну зміну, заміну або заряджання акумуляторів майже неможливою.

3. Поки дослідницьке співтовариство досліджує внесок відновлюваної енергії та механізмів самозаряджання, розмір вузлів все ще є стримуючим фактором.

4. Несправність кількох вузлів може призвести до передчасної фрагментації всієї мережі.

До проблеми споживання енергії можна підходити з двох сторін. Одною з них є розробка енергоефективних протоколів зв'язку (самоорганізація, протоколи доступу та маршрутизації), які враховують особливості БСМ. Інший підхід – визначити дії у мережах, які є одночасно марними та непотрібними, та зменшити їх вплив [3].

Марні та непотрібні дії можуть бути описані як локальні (обмежені вузлом) або глобальні (що мають масштаби всієї мережі). У будь-якому випадку, ці дії можуть бути розглянуті як випадкові побічні ефекти або результати неоптимальних програмних та апаратних реалізацій (конфігурацій). Наприклад, спостереження, що базуються на розгортанні у польових умовах, показують, що деякі вузли передчасно розряджали свої батареї через непередбачено активне та майже постійне прослуховування трафіку, що призвело до того, що підсистема зв'язку була змушена працювати довше, ніж передбачалося спочатку. Подібним

чином деякі вузли передчасно розряджали свої батареї, оскільки безцільно намагалися встановити зв'язок із мережею, яка стала для них вже недоступною.

Однак найбільш неефективні заходи є результатом неоптимальних конфігурацій апаратних та програмних компонентів. Наприклад, значна кількість енергії марно витрачається в режимі очікування обробки або в підсистемі зв'язку. Приймач, який безцільно приймає медіа дані або прослуховує спілкування сусідніх вузлів між собою, споживає значну кількість енергії.

Стратегія динамічного управління живленням (ДУЖ) забезпечує економічне споживання електроенергії. Стратегія може мати локальний або глобальний масштаб, або і те і інше. Локальна стратегія ДУЖ спрямована на мінімізацію споживання енергії окремими вузлами, забезпечуючи кожному підсистемі обсягом потужності, достатнім для виконання поставленого завдання. Коли немає завдання для обробки, стратегія ДУЖ змушує деякі підсистеми працювати у найбільш економічному режимі живлення або переводить їх у сплячий режим. Глобальна стратегія ДУЖ намагається мінімізувати загальне споживання електроенергії мережею, встановлюючи сплячий стан у всій мережі [3].

Існують різні способи досягнення цієї мети. Один із них – дозволити окремим вузлам визначати власні графіки сну та ділитися цими розкладами зі своїми сусідами, щоб забезпечити скоординоване зондування та ефективний зв'язок між вузлами. Це можна назвати синхронним сном. Проблема цього підходу полягає в тому, що сусідам також потрібно синхронізувати час та графіки, а це процес енергоємний. Інший спосіб – дозволити окремим вузлам дотримуватися власного графіку сну, а вузол, який ініціює спілкування, повинен надсилати запити доти, поки він не отримає підтвердження від свого приймаючого партнера. Цей підхід, відомий як асинхронний графік сну, дозволяє уникнути потреби в синхронізації графіків. Але це може мати побічний ефект на передачу даних. В обох підходах окремі вузли періодично прокидаються, щоб визначити, чи є вузол, який бажає спілкуватися з ними та обробити завдання, що очікують у черзі.

Першим кроком до розробки стратегії управління локальним живленням є розуміння того, як енергія споживається різними підсистемами безпроводового сенсорного вузла. Ці знання дозволяють уникати марних дій та економне витрачати енергію. Найбільш потужними споживачами є підсистема процесора та підсистема зв'язку.

У більшості існуючих підсистем обробки використовуються мікроконтролери, які можуть бути налаштовані на роботу в різних режимах живлення, наприклад, режим холостого ходу, зменшення шуму аналого-цифрового перетворювача, економії енергії, вимкнення живлення, очікування та розширеного режиму очікування. На додаток до вищезазначених конфігурацій, підсистема обробки може працювати з різними напругами живлення та тактовими частотами [3].

Хоча робота підсистеми процесора в різних режимах живлення є енергоефективною, перехід від одного режиму живлення до іншого також має власні витрати на споживання енергії та затримку. Ці втрати слід врахувати при

прийнятті рішення щодо обрання конкретного режиму живлення.

На споживання енергії підсистеми зв'язку можуть впливати кілька аспектів, включаючи тип модуляції, потужність підсилювача передавача та ефективність антени, діапазон, швидкість передачі та чутливість приймача. Деякі з цих аспектів можна динамічно переконфігурувати. Більше того, сама підсистема зв'язку може активувати або вимикати передавач та приймач, або обидва. Через наявність великої кількості активних компонентів, підсистема зв'язку (підсилювачі та генератори) споживає значну кількість струму в стані спокою, навіть якщо пристрій не працює.

Визначення найбільш ефективного режиму роботи в активному стані є не простим рішенням. Наприклад, споживання енергії передавача не обов'язково може бути зменшено простим зменшенням швидкості передачі або потужності передачі. Причина полягає в тому, що існує компроміс між корисною потужністю, необхідною для передачі даних, і потужністю, що розсіюється у вигляді тепла на підсилювачі потужності. Наприклад, трансивер Chipcon CC2420 має вісім програмованих рівнів вихідної потужності. Збільшення рівня потужності передачі на 24 дБ збільшує поточне споживання енергії лише вдвічі. Зазвичай, потужність розсіювання (теплова енергія) збільшується із зменшенням потужності передачі. Насправді більшість комерційно доступних передавачів ефективно працюють на одному або двох рівнях потужності передачі. Нижче певного рівня, ефективність підсилювача потужності різко падає. У деяких дешевих трансиверах, навіть у режимі максимальної потужності передачі, більше 60% живлення постійного струму розсіюється у вигляді тепла [3].

Додатковою проблемою енергопостачання є час, необхідний підсистемі зв'язку для переходу від неробочого режиму або режиму очікування до активного режиму. Перехід до режиму передачі відбувається з затримкою під час якої відбувається споживання енергії. Наприклад, фазове автопідстроювання частоти синтезатора передавача може вимагати до 300 мкс.

Таким чином, реалізація стратегії динамічного управління живленням в БСМ може значно збільшити термін життя як окремих сенсорів, так і мережі в цілому.

Література

1. Огляд методів підвищення ефективності мобільних безпроводових сенсорних мереж / Кравчук С.О., Явіся В.С., Лисенко О.І., Сушин І.О. // Начерк науково-практичної конференції «Сучасні системи зв'язку як напрям міжнародно-правової, зовнішньополітичної, теле-, радіо, мережевої комунікації»: збірник тез доповідей. Київ: ГО «УКРО», 2022. – С. 19-21. <https://www.doi.org/10.59105/2022-11>.
2. Явіся В.С., Лисенко О.І., Гетьман О.В. Критерії вибору алгоритмів керування потоками інформаційних повідомлень сенсорних мереж // Сімнадцята Міжнародна науково-технічна конференція «Перспективи телекомунікацій». Матеріали конференції. – К.: КПІ ім. Ігоря Сікорського. – 2023. – С. 317-319. <http://conferenc.its.kpi.ua/proc/article/view/282224>.
3. Fundamentals of wireless sensor networks: theory and practice / Waltenege Dargie, Christian Poellabauer. Wiley Series on Wireless Communications and Mobile Computing, 2010. – 311 pp. ISBN 978-0-470-99765-9.

ПРАВИЛА ПОБУДОВИ ТРАЄКТОРІЇ ПОЛЬОТУ КОМУНІКАЦІЙНОЇ АЕРОПЛАТФОРМИ ДЛЯ ЗБОРУ ДАНИХ З ВУЗЛІВ БЕЗПРОВОДОВОЇ СЕНСОРНОЇ МЕРЕЖІ

Романюк В.А., Гримуд А.Г.

Військовий інститут телекомунікацій та інформатизації, Україна

E-mail: romval2016@gmail.com

RULES FOR CONSTRUCTING THE FLIGHT TRAJECTORY OF A COMMUNICATION AIRPLANE PLATFORM FOR DATA COLLECTION FROM WIRELESS SENSOR NETWORK NODES

Options have been proposed for the formation of rules for constructing the flight path of a communication aerial platform for collecting data from nodes of a wireless sensor network to optimize the time of data collection and the operating time of network nodes.

Розглядається безпроводова сенсорна мережа (БСМ) з незв'язними стаціонарними вузлами, які розташовані на важкодоступній території при відсутності будь-якої комунікаційної інфраструктури. БСМ має значну розмірність (сотні, тисячі вузлів) та обмежені ресурси вузлів (енергія батареї, продуктивність процесора, обсяг пам'яті, потужність передавача, тощо). Збір інформації моніторингу з вузлів БСМ в умовах відсутності зв'язності між ними можливий тільки з застосуванням комунікаційної аероплатформи (КА), яка побудована на базі БПЛА. Сенсорні вузли здійснюють збір даних про параметри зовнішнього середовища (об'єктів, цілей) зон моніторингу, їх збереження та подальшу передачу до комунікаційної аероплатформи при наявності з нею радіозв'язності.

Основними цільовими функціями процесу збору даних КА з вузлів БСМ можуть бути: мінімізація часу (граничний час) збору даних, максимізація часу (визначений час) функціонування мережі [1, 2]. Досягнення цих оптимізаційних задач залежить від прийнятого рішення по траєкторії польоту КА для збору даних з вузлів мережі.

Найпростіше рішення по траєкторії КА – реалізувати обліт всієї площі розташування вузлів БСМ (фактично реалізується при первинному обльоті) за певними алгоритмами (правилами): за смугами (вертикальними або горизонтальними), за периметром, тощо. Однак таке рішення призводить до значного часу обльоту вузлів мережі КА. Другий спосіб – віртуальна кластеризація мережі, визначення в кластерах точок збору даних (зазвичай в центрі кластеру) та побудова траєкторії польоту КА між точками збору.

В роботах [1, 2] запропонована ієрархія рішень (алгоритмів, правил) по досягненню визначених цільових функцій за рівнями: вся мережа, конкретний кластер, КА-група вузлів, КА-окремий вузол.

На мережевому рівні досягнення цільових функцій відбувається (рис. 1):

1. Оптимізацією розмірів зони покриття R (шляхом визначення висоти польоту КА, діаграми спрямованості антени). Проводиться віртуальна однорідна кластеризація мережі з адаптацією фіксованого розміру кластерів

(використовується алгоритм кластерного аналізу FOREL) з врахуванням координат вузлів, їх взаємного розташування та пріоритету цільових функцій.

2. Оптимізацією кількості віртуальних кластерів, яка досягається застосуванням множини правил об'єднання (роз'єднання) кластерів, правил визначення точок формування та перебору кластерів.

3. Визначенням кращого евристичного алгоритму пошуку найкоротшого маршруту обльоту КА центрів кластерів з визначеної множини (наприклад, за клітинками, опуклої оболонки, найближчого сусіда тощо). Кожен з цих алгоритмів має свої параметри оптимізації. Так для алгоритму пошуку найкоротшого маршруту обльоту КА за клітинками пропонується проводити оптимізацію розмірів клітинок, випуклої оболонки – її розміру, найкоротшого маршруту – кількості найкоротших ділянок (1...5, обмеження пов'язано зі значним збільшенням перебору варіантів із-за обчислювальної складності алгоритму).



Рис. 1. Етапи синтезу правил побудови траєкторії польоту КА для збору даних з вузлів БСМ

4. Визначенням кількості та локації точок (інтервалів) для обміну при зависанні (в русі) КА для збору даних з врахуванням: параметрів груп вузлів та окремих вузлів (взаємне розташування відносно траєкторії, наявна енергія вузлів, обсяг даних моніторингу), пріоритету цільових функцій тощо [1].

Основними способами визначення точок є:

- при побудові ділянки траєкторії КА між кластерами відразу будуються точки (інтервали) обміну вузлів на цієї ділянці траєкторії;
- побудова точок (інтервалів) обміну відбувається після формування всієї траєкторії (фактично враховується можливість розташування вузла ближче до будь-якої іншої ділянки траєкторії);
- врахування наближеності вузла до певного центру кластера.

Для оцінки ефективності можливих варіантів формування правил побудови траєкторії КА на мові Python розроблена відповідна імітаційна модель процесу збору даних з вузлів БСМ з використанням КА.

Для моделювання визначені наступні вхідні дані.

1. Характеристики мережі, вузлів, КА:

- форма (прямокутник, коло, смуга) та розмір площі розташування вузлів БСМ, їх кількість, тип (однорідний, з групуванням) та координати розміщення; обсяг зібраних даних моніторингу кожним вузлом та інтенсивність збору тощо;

- технічні характеристики вузла – кількість та типи сенсорних датчиків, рівень енергії батареї, витрати енергії на моніторинг параметрів середовища (об'єктів) для кожного типу датчика тощо;

- комунікаційні характеристики вузла – параметри антени, прийомопередавача, витрати енергії на біт прийому та передачу даних для обраного MAC-протоколу, відстані та типу обладнання тощо;

- польотні характеристики КА (БПЛА) – тип, швидкість, висота, час та дальність польоту, енергія батареї, витрати енергії на рух та інформаційний обмін, можливість зависання та переміщення у просторі тощо;

- комунікаційні характеристики КА – MAC-протокол, параметри антени, прийомопередавача, обсяг пам'яті та ін.

2. Множина алгоритмів (правил) мережевої оптимізації згідно розглянутих варіантів їх формування:

- алгоритм кластеризації мережі (FOREL) з множиною правил оптимізації розмірів та кількості кластерів, вибору точок визначення кластерів;

- алгоритми пошуку найкоротшого маршруту (найближчого сусіда, клітинок, зовнішньої оболонки з відповідними параметрами оптимізації), тощо;

- правила визначення точок (інтервалів) збору даних в русі на траєкторії польоту КА (в процесі та після побудови траєкторії, з врахуванням зависання в центрах кластерів тощо).

В результаті моделювання отримано залежності часу збору даних, часу функціонування мережі від вхідних параметрів мережі та множини правил побудови траєкторії КА. Крім цього модель дозволила дослідити: параметри оптимізації при кластеризації (кількість та розміри кластерів, варіанти), правила знаходження точок (інтервалів) збору даних на траєкторії польоту КА, параметри оптимізації алгоритмів пошуку найкоротшого маршруту тощо.

Таким чином, результати моделювання показали, що єдиної універсальної множини правил не існує. Досягнення раціонального рішення по траєкторії КА буде відбуватися за ієрархією (згідно цільової функції) з визначеної множини правил. Розроблена імітаційна модель процесу збору даних КА з вузлів БСМ працює в режимі близькому до реального часу, дозволяє провести оцінку ефективності застосування правил та може бути використана як на етапі проектування системи управління КА, так і на етапі оперативного управління.

Література

1. Romaniuk V., Hrymud A. A model of situational control of the telecommunication aerial platform flight trajectory to collect data from nodes of a wireless sensor network. Communication, informatization and cybersecurity systems and technologies, 2023. № 3. p. 88 – 100. DOI: 10.58254/viti.3.2023.12.101.
2. Romaniuk V., Hrymud A. Analysis of the rules for constructing a flight trajectory of a communication aerial platform for data collection from nodes of a wireless sensor network. Communication, informatization and cybersecurity systems and technologies, 2023. № 4. p. 65 – 81. DOI: 10.58254/viti.4.2023.06.65.

ВИКОРИСТАННЯ ПІДХОДУ ІОТ ЯК ПЕРСПЕКТИВНИЙ НАПРЯМ РОЗВИТКУ ПЕРВИННОЇ ДІАГНОСТИКИ СТАНІВ ЛЮДИНИ

Коваленко І.Л., Мовчанюк А.В.

Радіотехнічний факультет КПІ ім. Ігоря Сікорського,

Siemens Healthineers AG Україна

E-mail: igor.kovalenko@siemens-healthineers.com

USE OF THE IOT APPROACH AS A PROMISING TREND FOR THE DEVELOPMENT OF PRIMARY DIAGNOSTICS OF HUMAN HEALTH

The article studies the development of the field of primary diagnostics of human health with the help of personal use devices as a promising area of Internet of Things. The practical approaches used in the creation of a commercial IoT device for the current monitoring of a woman's fertile period are considered.

Проведено дослідження розвитку галузі первинної діагностики стану здоров'я людини за допомогою пристроїв персонального використання, як перспективного напрямку Internet of Things. Розглянуто практичні підходи використані під час створення комерційного IoT пристрою для поточного моніторингу фертильного вікна жінки.

За останні 10 років спостерігається суттєве зростання інтересу до використання підходу компактних пристроїв в галузі охорони здоров'я, особливо в первинній діагностиці та моніторингу станів людини [1]. Цей інтерес визначається загальним характером зміни клініко-центричних тенденцій в бік пацієнто-центричного підходу. Компактні Internet-of-Things (далі IoT) пристрої, такі як розумні годинники, браслети, кільця та інші датчики, надають можливість неперервного відстеження різних вітальних показників, таких як пульс, тиск, рівень кисню в крові, надаючи користувачам зручний і доступний інструмент для поточного моніторингу здоров'я, без необхідності відвідування лабораторії чи клініки. З іншого боку, наявність неперервного і тривалого моніторингу різних показників може дати лікарю комплексну та більш об'єктивну картину, аніж одиничний лабораторний аналіз, особливо враховуючи можливість передачі даних в електронному вигляді. Таким чином, завдяки широкому розповсюдженню та доступності цих пристроїв, пацієнти можуть ефективно взаємодіяти з системою охорони здоров'я, забезпечуючи додаткові дані для аналізу та лікування.

Згідно з проведеними маркетинговими дослідженнями [1] тенденція збережеться в найближчі роки по всім регіонам з щорічним збільшенням темпів зростання об'єму ринку, рис.1. Прогнозується також поява суттєвого попиту на перспективних ринках країн Латинської Америки та Африки.

Окремим чинником, який варто зазначити – це те, що популяризація носимих діагностичних пристроїв створила велику базу медичних даних, яка може бути проаналізована системами машинного навчання та штучного інтелекту, що вже зараз дозволяє здійснювати ранню діагностику різних захворювань та виявляти аномалії в роботі органів та систем людини.

У цьому контексті важливо розуміти переваги та виклики використання підходу IoT-пристроїв в галузі первинної діагностики та розвивати нові стратегії для їх зручного використання в щоденному житті.

Об'єм ринку компактних медичних пристроїв,
по регіонам, 2019 - 2031,
(мільярд американських доларів)



Джерело: Polaris Market Research Analysis

Рис. 1. Об'єм ринку компактних медичних пристроїв,
нинішній стан та прогноз по регіонам.

Застосування IoT в первинній діагностиці.

Розвитку галузі компактних діагностичних пристроїв передувала ціла низка факторів та чинників – як технологічних, так і суспільних.

Створення компактних пристроїв було б неможливе без технологічних досягнень – розвитку мікроелектроніки та компонентної бази, зростання рівня інтеграції, поліпшення ефективності використання та ємності малогабаритних елементів живлення. Необхідними передумовами створення IoT як галузі були активний розвиток персональних електронних пристроїв та мобільних мереж передачі даних. Серед соціальних передумов швидкого набуття популярності компактних пристроїв діагностики та моніторингу станів здоров'я варто відзначити тенденцію до збільшення інтересу суспільства розвинених країн до здорового способу життя та самостійного ведення власного здоров'я, що, відповідно, збільшило попит на зручні та доступні засоби первинної самодіагностики та спостереження життєвих показників.

Ці та інші фактори створили сприятливе середовище для інтенсивного розвитку носимих медичних та діагностичних пристроїв, які, в свою чергу, є підгрупою більш широкого класу IoT.

Запропонована [2] узагальнена класифікація медичних та діагностичних IoT-пристроїв, що базується на їх застосуванні:

- дистанційна медицина – бездротові IoT рішення для безпечного збору даних пацієнта, їх первинну обробку та передачу кваліфікованому спеціалісту для надання рекомендацій;
- поточний моніторинг – персональні сенсори неінвазивного моніторингу станів людини з режимі реального часу;
- пристрої профілактичної медицини – IoT медичні системи, що використовують дані з датчиків для раннього виявлення та попередження аномалій та хворобливих станів.

Як вже частково було зазначено у вступній частині, підхід Інтернету Речей має широкий спектр аспектів, що можуть бути корисними у сфері медицини. Тривале відстеження вітальних показників у реальному часі дає важливі дані динамічних змін в залежності від різних факторів, що можуть бути використані для ранньої діагностики вікових змін, хвороб внутрішніх органів чи порушень обміну речовин. Аналізуючи сукупні характеристики життєвих показників можна відслідкувати навіть деструктивні зміни у психологічних станах, таких як депресія [3] чи тяжкий перебіг стресу [4]. Рання діагностика та прогнозування дають

можливість вчасно прийняти відповідні заходи. Завдяки IoT можливий віддалений моніторинг пацієнтів. Це особливо важливо для людей з хронічними захворюваннями, які можуть отримувати медичний нагляд зручно та ефективно. Аналіз даних, зібраних за допомогою персональних пристроїв, дозволяє виробити персоналізовані терапії та підходи до лікування на основі індивідуальних особливостей пацієнта [5].

На ефективність використання підходів IoT для покращенні діагностики, моніторингу та загального управління системами охорони здоров'я вказують результати численних наукових досліджень. Було проведено як систематичні узагальнені дослідження позитивного впливу поточної діагностики здоров'я за допомогою компактних пристроїв на покращення результатів лікування пацієнтів [6], так і розглянуто конкретні випадки застосування певних пристроїв для ранньої діагностики захворювань [7], з оцінкою їх ефективності в порівнянні зі звичайними методиками.

Результати досліджень вказують на широкий спектр застосувань IoT у медицині та переконливо демонструють його перспективність у покращенні первинної діагностики.

Практичний досвід провадження інноваційних підходів у моніторингу фертильності.

Проблематика: За даними звіту Всесвітньої організації охорони здоров'я [8] 19% жінок у віці від 19 до 49 років мають складнощі з першою вагітністю через проблеми з фертильністю, по причині чого вдаються до різних методів відслідковування фертильного вікна – короткого фізіологічного періоду зрілості яйцеклітини, коли можливість завагітніти найвища.

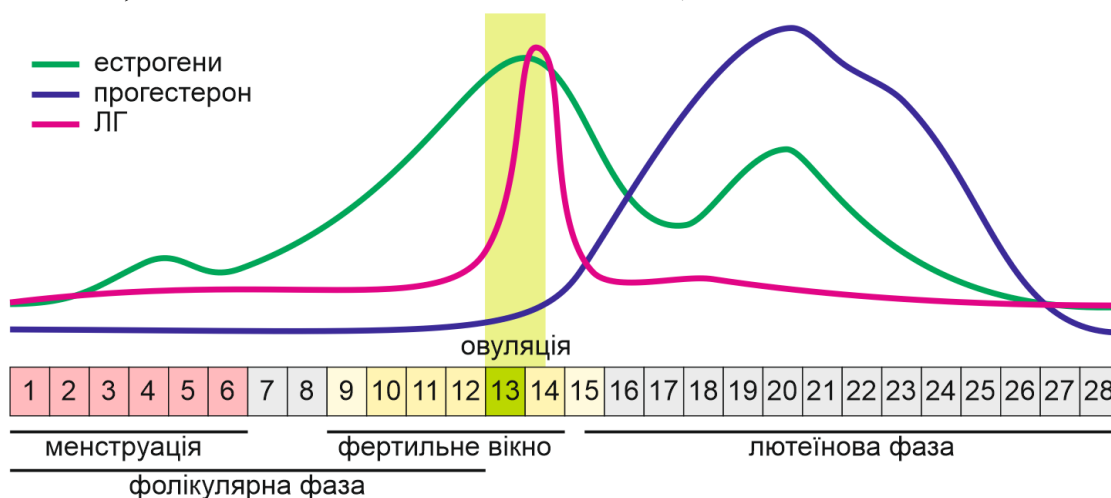


Рис. 2. Фертильне вікно та овуляція у менструальному циклі.

Методологія: Існує декілька розповсюджених методик відслідковування овуляції, основні з яких це:

- календарний метод - ґрунтується на регулярності циклу і теоретичній моделі. Недолік – низька точність, оскільки регулярність циклу є індивідуальною характеристикою, на яку впливає велика кількість факторів;

- бтт-метод – ґрунтується на вимірюванні базальної температури тіла (бтт), яка може незначно підвищитися через вивільнення прогестерону. Недолік – необхідна висока точність датчиків, щоб зафіксувати зміну температури, значний вплив зовнішніх факторів.

- овуляційні тести – ґрунтуються на визначенні рівню лутеїнізуючого гормону (ЛГ), який підвищується приблизно за 24 години перед овуляцією. Недолік – незручні у використанні, дають позитивний результат лише в день піку овуляції.

Задача: створити компактний пристрій, що буде простим і зручним у використанні та матиме переваги IoT підходу.

Під час детального опрацювання питання були вивчені наукові дослідження щодо альтернативних методик відслідковування овуляції – серед яких аналіз рівня кристалізації слини при висиханні. Збільшення рівня вільних естрогенів у рідинах організму жінки під час овуляції викликає специфічну картину кристалізації зразків слини, схожу на листя папороті.

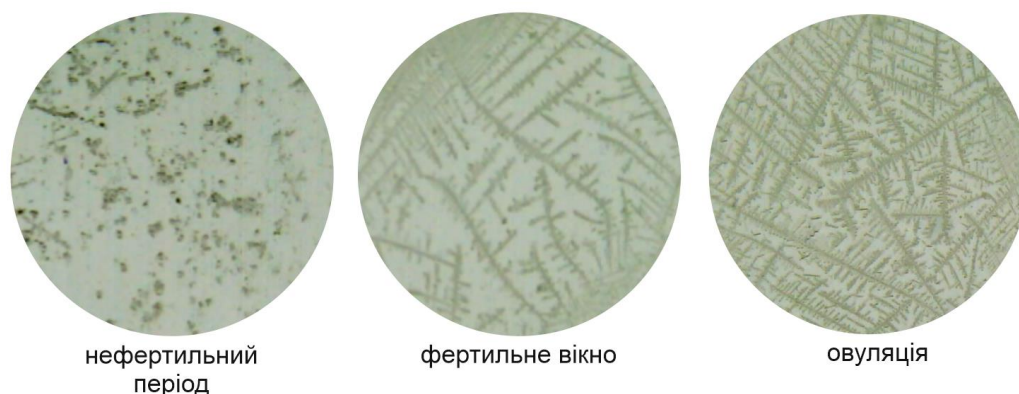


Рис. 3. Характер кристалізації слини в залежності від періоду менструального циклу.

Навіть враховуючи високу точність у понад 99% [9] метод не набув популярності через необхідність використання оптичного мікроскопу та потребу у спеціальних навичках. Використовуючи сучасну елементну базу, алгоритми машинного навчання та підходи IoT вдалося створити пристрій, що позбавлений цих недоліків.

Для стабільного та якісного виявлення папороте-подібних кристалів у зразках висохлої слини була розроблена та досліджена спеціалізована оптична система, що в парі з джерелами пружного світлорозсіяння (англ. elastic light scattering) дала змогу робити контрастні знімки високої роздільної здатності, які гарно піддаються аналізу за допомогою алгоритмів машинного навчання.

Під час дослідної експлуатації був зібраний унікальний датасет знімків, що дав можливість створити алгоритм коректного розпізнання кристалізації з вірогідністю 96,2%.

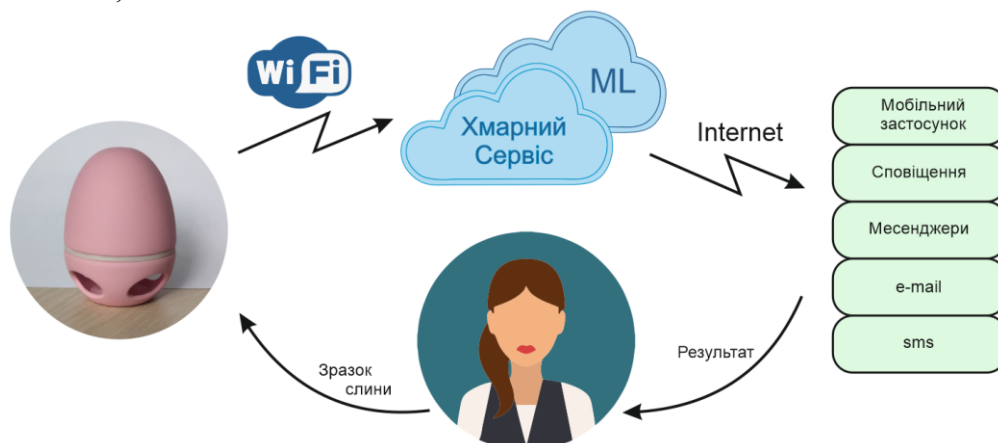


Рис. 4. IoT підхід у пристрої відслідковування фертильного вікна.

ML-алгоритми потребують значних обчислювальних потужностей і великих об'ємів пам'яті для накопичення датасетів, що стало причиною вибору вектору IoT і хмарних обчислень. За понад рік розробки і дослідної експлуатації цільовою групою пристрій декілька разів видозмінювався і набув сучасного вигляду – автономного компактного аналізатору з прямим підключенням до мережі WiFi та глибокою інтеграцією у хмарні сервіси та мобільний застосунок. Щоденне використання пристрою дає можливість відслідковувати фертильне вікно весь період його тривалості, в незалежності від зовнішніх факторів та індивідуальних особливостей. Забір зразку займає всього декілька секунд часу користувача і не викликає дискомфорту чи незручностей, не вимагає спеціального обладнання чи навичок. Всі інші кроки проведення аналізу приховані від користувача і не потребують його залучення. Після висихання зразку аналізатор в повністю автоматичному режимі робить серію знімків використовуючи вбудовану систему підсвітки і проводить первинну обробку зображення для досягнення високої контрастності та зменшення об'єму даних, що передаються по мережі, і надсилає результат хмарному сервісу, де з використанням алгоритмів машинного навчання визначається рівень кристалізації, у відповідності до якого користувачка отримує фінальний висновок у зручний для неї спосіб – через мобільний застосунок, месенджери чи повідомлення.

Слідування концепції IoT дало можливість створити водночас функціональний і компактний аналізатор, який поєднує в собі простоту використання і точність досліджень, не має розхідних матеріалів, повністю автономний і доступний.

Література

1. Wearable Medical Device Market Share, Size, Trends, Industry Analysis Report, By Device Type (Diagnostic Device And Therapeutic Device); By Application; By Distribution channel; By Region; Segment Forecast, 2024- 2032.; 2023, <https://www.polarismarketresearch.com/industry-analysis/wearable-medical-devices-market>.
2. Abdulmalek S, Nasir A, Jabbar WA, Almuhaya MAM, Bairagi AK, Khan MA-M, Kee S-H. IoT-Based Healthcare-Monitoring System towards Improving Quality of Life: A Review. *Healthcare*. 2022; 10(10):1993.
3. Nickson D, Meyer C, Walasek L, Toro C. Prediction and diagnosis of depression using machine learning with electronic health records data: a systematic review. *BMC Med Inform Decis Mak*. 2023 Nov 27;23(1):271. doi: 10.1186/s12911-023-02341-x. PMID: 38012655; PMCID: PMC10680172.
4. Kang M, Chai K. Wearable Sensing Systems for Monitoring Mental Health. *Sensors (Basel)*. 2022 Jan 27;22(3):994. doi: 10.3390/s22030994. PMID: 35161738; PMCID: PMC8839602.
5. Frimpong, Bismark Atta & Barbosa, Claudia & Alhameed, Raed. (2023). The Impact of the Internet of Things (IoT) on Healthcare Delivery: A Systematic Literature Review. *Journal of Techniques*. 5. 84-91. 10.51173/jt.v5i3.1433.
6. Himanshu Verma, Naveen Chauhan, Lalit Kumar Awasthi, A Comprehensive review of 'Internet of Healthcare Things': Networking aspects, technologies, services, applications, challenges, and security concerns, *Computer Science Review*, Volume 50, 2023, 100591, ISSN 1574-0137.
7. M. N. Bhuiyan, M. M. Rahman, M. M. Billah and D. Saha, "Internet of Things (IoT): A Review of Its Enabling Technologies in Healthcare Applications, Standards Protocols, Security, and Market Opportunities," in *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10474-10498, 1 July1, 2021, doi: 10.1109/IJOT.2021.3062630.
8. World Health Organization, Sexual and Reproductive Health and Research (SRH), «Infertility Prevalence Estimates, 1990–2021», Global report, 3 April 2023, <https://www.who.int/publications/i/item/978920068315>
9. Potluri V, Kathiresan PS, Kandula H, Thirumalaraju P, Kanakasabapathy MK, Kota Sai Pavan S, Yarravarapu D, Soundararajan A, Baskar K, Gupta R, Gudipati N, C Petrozza J, Shafiee H. An inexpensive smartphone-based device for point-of-care ovulation testing. *Lab Chip*. 2018 Dec 18;19(1):59-67. doi: 10.1039/c8lc00792f. PMID: 30534677; PMCID: PMC6321627.

АРГУМЕНТАЦІЯ ПОЄДНАННЯ БПЛА ТА БСМ ДЛЯ ДИСТАНЦІЙНОГО ЗОНДУВАННЯ НЕБЕЗПЕЧНИХ РЕЧОВИН

Карпенко М.І., Чумаченко С.М., Мошенський А.О.

Національний університет харчових технологій, м. Київ, Україна

E-mail: sapta@ukr.net

ARGUMENTATION OF THE CONNECTION OF UAVS AND WSN FOR REMOTE SENSING OF DANGEROUS SUBSTANCES

This article considers the prospects of using unmanned aerial vehicles (UAV) and wireless sensor networks (WSN) of the Internet of Things (IoT) for remote sensing of dangerous substances. In the context of contemporary realities in the form of Russian terrorist attacks with the use of chemical weapons and shelling of nuclear power plants, the author emphasizes the advantage of UAVs in identifying and monitoring dangerous substances. The article proposes the combination of UAVs and WSN into a single network and shows the results of the analysis of possible methods and means of communication of WSN network devices.

Дистанційне виявлення небезпечних речовин покладено на війська РХБЗ. Виділяють радіаційну, хімічну та біологічну розвідки. Кожна з них проводиться по-своєму та має власний набір методів та засобів щодо виявлення та розпізнавання небезпеки. Радіаційна та хімічні розвідки проводяться як наземно, так і в повітрі. Наземний тип розвідки передбачає наявність засобів виявлення та розпізнавання. Більшість із цих засобів є старими зразками радянських часів. Наприклад, для радіаційної розвідки характерна наявність таких спеціальних засобів: індикатори (ДП-63, ДП-63А, ДП-64), вимірювачі потужності дози (ДП-5В, ДП5ВБ(А,Б,В), ИМД-5, ИМД-1, ДБГ-06Т, ИМД-21Б, ИМД-31), вимірювачі дози (ДП-22В, ДП-24, ИД-11), комплекси дозиметрів (ИД-1, ИД-11, ДК-0,2), дозиметри-радіометри (МКС-05, МКС-У, ДП-12, ДП-100М, ДП-100АДМ, «Луч-А», «Тиса»), дозиметричні установки (КДУ-6Б), а також прилади радіаційної та хімічної розвідки (ПРХР, ПРХР-МЕ) [1]. Однак, є і нові зразки, на кшталт блоків детектування БДБГ-Т виробництва тм. ЕКОТЕСТ, що встановлюються на наземну техніку. Хімічна розвідка також має наземну техніку у вигляді БРДМ-РХ, УАЗ-469-РХ, БТР-РХ. Повітряний моніторинг здійснюється за допомогою літальних апаратів на кшталт БЛР оп "Стриж", БЛР "Рейс". Дана ситуація у вигляді здійснення моніторингу ручними засобами (дозиметрами, радіометрами, і т.п.) та встановленими на наземну техніку приладами (блоки детектування, хім лабораторії і т.п.) показує нам необхідність популяризації застосування БПЛА. Переваги дистанційного зондування перед звичайним беззаперечні, оскільки усувається необхідність наражати людину на небезпеку знаходження в зонах забруднення, небезпечних для життя. Тим паче, що точність вимірювання від цього значно зростає [2]. Наземна техніка краще вберігає екіпаж від шкідливого середовища, однак повне перенесення блоків детектування на БПЛА дало б змогу повністю ізолювати оператора від

шкідливих впливів та значно пришвидшити обстеження заражених зон.

Ручні та стаціонарні дозиметри вкрай рідко мають знімні носії для запису отриманої інформації, ще рідше вони мають канал зв'язку, по якому вони передають дані дистанційно. З бортовими приладами ситуація краще, але все одно вони зазвичай мають закриту мережу для кількох блоків. Створення динамічної БСМ підвищило б ефективність моніторингу на порядок. Цей факт доводить підписання Міноборони України Меморандуму про співпрацю з аналітичним проєктом DeepStateUA, який публікує карту з оновленнями щодо перебігу бойових дій в Україні. Маршрути для БПЛА можна побудувати [3] та використовувати дані точок вимірювання у реальному часі. Це стане можливим за допомогою включення БПЛА в мережу IoT як рухомого датчика, обладнаного необхідними сенсорами та радіо модулями [4].

Подібна мережа може бути сформована на основі безпроводового каналу передачі даних повнозв'язної топології мережі або mesh в УКХ діапазоні.

Ультракороткі хвилі мають діапазон 300 МГц - 3 ГГц і є ідеальним вибором за рахунок кількох факторів: можливість передавати велику кількість даних на великі відстані; коротка довжина хвилі дозволяє зменшити розміри антен та модулів, що важливо для створення блоку з модулів для розміщення їх на БПЛА за рахунок зменшення розміру та ваги блоку пристроїв; радіосигнали на ультрависоких частотах мають хорошу проникність через перешкоди, що дозволяє передавати дані через стіни та інші перешкоди без значного зниження якості сигналу; передача числової інформації датчиків не потребує такої широкої смуги пропускання, що дозволяє уникнути необхідності використання діапазонів радіохвиль з вищою пропускнуою здатністю для передачі фото та відео.

Mesh та повнозв'язна мережа забезпечить створення зон суцільного інформаційного покриття великої площі, масштабованість та стійкість мережі до втрати окремих елементів.

Для забезпечення роботи мережі типу mesh (яка вимагається нашим проєктом) необхідно обрати радіомодуль, який підтримує відповідні протоколи LPWAN. LPWAN (Low-Power Wide-Area Network) - це група протоколів зв'язку, які дозволяють передавати дані на великі відстані з мінімальним використанням енергії. Відомі наступні протоколи LPWAN: LoRa, SIGFOX, NB-IoT або LTE-M.

Підхід, що використовується передачі даних в LPWAN-мережі, схожий принцип роботи стільникових мереж. Розумні датчики або лічильники передають сигнал радіоефіру. Базові станції приймають та оцифровують сигнали від LPWAN-пристроїв, передаючи їх далі на сервер. На серверах дані від усіх станцій у мережі обробляються та надаються у зручному для користувача вигляді. Зворотній зв'язок дозволяє керувати пристроями віддалено.

Згідно з матеріалів порівнянь технологій радіозв'язку у праці Топал, О.І. та ін., найкращою для наших потреб є технологія LoRa, яка базується на

технології розширення спектру (Spread Spectrum Modulation) та варіації лінійної частотної модуляції (Chirp Spread Spectrum, CSS), що дозволяє забезпечити високу стійкість зв'язку на великих відстанях.

Для формування мережі УКХ діапазону кожному з модулів для збору даних необхідний трансивер. Від якості трансивера залежать параметри зв'язку, такі як чутливість, максимальна потужність передачі, дальність зв'язку, швидкість передачі даних тощо. Найпопулярнішими виробниками трансиверів є Semtech, Texas Instruments, Microchip Technology, STMicroelectronics, Silicon Labs, RF Solutions, HopeRF, Murata. Найвищу дальність мають радіомодулі з підтримкою протоколу LoRaWAN (частота, швидкість передачі, дальність зв'язку): Ra-06(410-525МГц, 300Кб/с, 5км), RFM95W (868МГц, 300Кб/с, 8км), Lora32u4 II (868-915 МГц, 300Кб/с, 4-7.2км), N533LS (868-915МГц, 2000 Кб/с, 14км). Усі названі радіомодулі мають малі габарити (від 16×16 у RFM95W до 53×25 в Lora32u4 II) та доволі високі ціни (438,670, 514 грн в Ra06, Lora32u4 II та N533LS відповідно), окрім RFM95W, який можна знайти на ринку за 271 грн станом на 17.03.2023[6].

Розглянуто перспективи використання безпілотних літальних апаратів, підкреслено перевагу БПЛА у визначенні та моніторингу небезпечних речовин, показано результати аналізу можливих методів та засобів комунікації пристроїв мережі БСМ.

Література

1. Чернявський І. Ю., Марущенко В. В., Мартинюк І. М. (2022). Військова дозиметрія: підручник. К. : Вид. «КНТ», 530 с. ISBN 978-966-570-818-6.
2. Connor, D., Martin, P. G., & Scott, T. B. (2016). Airborne radiation mapping: overview and application of current and future aerial systems. *International journal of remote sensing*, 37(24), 5953-5987.
3. Чумаченко, С. М., et al. "42. МЕТОД ЗБОРУ ІНФОРМАЦІЇ ПРО СТАН ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ З ВУЗЛІВ БЕЗПРОВОДОВОЇ СЕНСОРНОЇ МЕРЕЖІ." CHALLENGES AND THREATS TO CRITICAL INFRASTRUCTURE (2023): 171.
4. Лисенко, О. І., Тачиніна, О. М., Пономаренко, С. О., & Гуйда, О. Г. (2023). Теорія оптимальних розгалужених траєкторій.
5. Топал, О.І., Любарець, М.І., Прищепов Є.О. (2020) ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ ОБЛІКУ СПОЖИВАННЯ ЕНЕРГЕТИЧНИХ РЕСУРСІВ: СКЛАДНИКИ, ТЕХНОЛОГІЇ РАДІОЗВ'ЯЗКУ ТА ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ В УКРАЇНІ, ВЧЕНІ ЗАПИСКИ ТАВРІЙСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ІМЕНІ В.І. ВЕРНАДСЬКОГО Серія: Технічні науки Том 31 (70) № 6 2020 Частина 1 сторінка 31.
6. Карпенко, М.І., Чумаченко, С.М., Мошенський, А.О. (2023) Вибір оптимального способу передачі даних для створення програмноапаратного комплексу інформаційної системи виявлення небезпечних речовин. *International scientific conference of young scientist and students "Youth scientific achievements to the 21st century nutrition problem solution"*, April, 3-7, 2023. Book of abstract. Part 2. NUFT, Kyiv.

ГРАНИЧНІ ОБЧИСЛЕННЯ В ІНТЕРНЕТІ РЕЧЕЙ: ЛОКАЛЬНИЙ АНАЛІЗ ТА УПРАВЛІННЯ ЕНЕРГІЄЮ

Корнійчук І. Г., Курдеча В.В.

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна
E-mail: korniichuk2002@gmail.com*

EDGE COMPUTING IN THE INTERNET OF THINGS: LOCAL ENERGY ANALYSIS AND MANAGEMENT

Edge computing in the context of the Internet of Things allows for localized energy analysis and management by moving computing and data storage closer to where it is used. This improves system efficiency, reduces latency, and allows for faster response to changing conditions, which helps to optimize energy use and improve reliability.

Граничні обчислення, які наближають обчислення і зберігання даних до місця їх використання, відкривають нові горизонти в енергетичному секторі. Ця технологія дозволяє оптимізувати операції, знижувати витрати і підвищувати надійність, роблячи енергетичні системи більш ефективними і надійними.

Використовуючи граничні обчислення для моніторингу та управління системами генерації та розподілу енергії в режимі реального часу, енергетичні компанії можуть зменшити затримки, покращити час реагування та підвищити обізнаність про ситуацію. Це дозволяє їм швидше виявляти проблеми і реагувати на них, що призводить до підвищення надійності і скорочення часу простою. Приклад такої системи зображено на рисунку 1.1.

Аналізуючи дані на межі мережі, енергетичні компанії можуть виявити неефективність і оптимізувати використання енергії. Це може призвести до економії коштів і поліпшення стійкості, а також підвищення ефективності та надійності.

Обробляючи дані локально, енергетичні компанії можуть знизити ризик кібератак і захистити конфіденційні дані від несанкціонованого доступу. Це може підвищити надійність і безпеку енергетичних систем, а також захистити конфіденційність споживачів.

Граничні обчислення можуть сприяти оптимізації інтеграції відновлюваних джерел енергії в енергосистему. Обробляючи дані локально, енергетичні компанії можуть аналізувати дані про виробництво і споживання енергії в режимі реального часу і відповідно коригувати роботу мережі. Це може призвести до підвищення стабільності та надійності мережі, а також збільшення використання відновлюваних джерел енергії.

Нарешті, граничні обчислення відкривають нові можливості для енергетичних послуг та бізнес-моделей. Обробляючи дані локально, енергетичні компанії можуть пропонувати нові послуги та додатки, які раніше були неможливі. Наприклад, вони можуть пропонувати моніторинг

використання енергії в режимі реального часу і зворотній зв'язок зі споживачами, або уможливити пірингову торгівлю енергією.

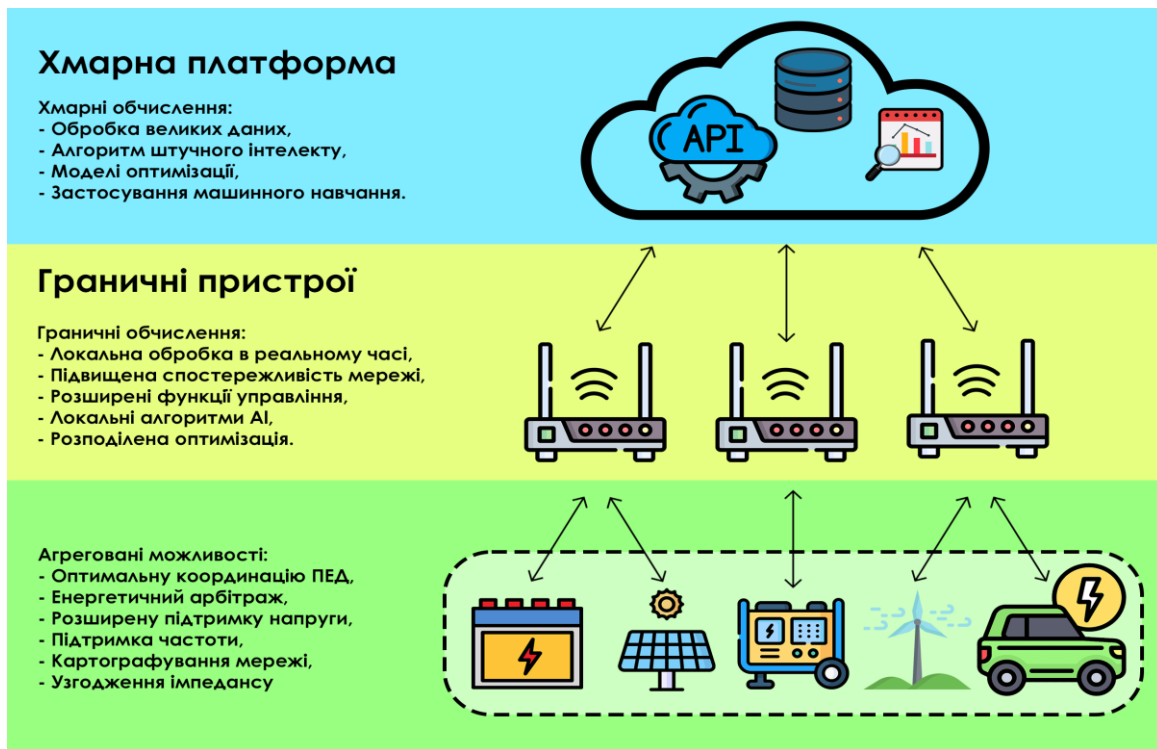


Рис. 1. Схематичне представлення системи (Edge Computing).

Периферійні обчислення в енергетичному секторі відкривають нові можливості для моніторингу та управління в режимі реального часу. Ця технологія, яка переміщує обчислення та зберігання даних ближче до місця їх використання, дозволяє енергетичним компаніям швидше виявляти проблеми, реагувати на них та підвищувати надійність енергосистем.

Використання периферійних обчислень для моніторингу та управління системами виробництва, передачі та розподілу енергії в режимі реального часу дозволяє енергетичним компаніям швидше виявляти та вирішувати проблеми. Наприклад, вони можуть використовувати цю технологію для моніторингу продуктивності вітрових турбін або сонячних панелей в режимі реального часу, а також для моніторингу стану ліній електропередач, трансформаторів та інших компонентів енергосистеми.

Однією з ключових переваг моніторингу та управління в режимі реального часу є покращення обізнаності про ситуацію. Завдяки локальній обробці даних енергетичні компанії можуть швидко виявляти проблеми та реагувати на них, що призводить до підвищення надійності, скорочення часу простою та підвищення безпеки для працівників і споживачів.

Моніторинг і управління в режимі реального часу також можуть сприяти оптимізації використання енергії. Аналізуючи дані про виробництво та споживання енергії в режимі реального часу, енергетичні компанії можуть коригувати роботу мережі для забезпечення більш ефективного використання енергії. Наприклад, вони можуть регулювати потужність вітрових турбін або сонячних панелей на основі поточного попиту на енергію або регулювати потік електроенергії через мережу, щоб зменшити втрати.

Нарешті, периферійні обчислення дозволяють проводити прогнозоване технічне обслуговування. Аналізуючи дані про продуктивність енергетичних систем в режимі реального часу, енергетичні компанії можуть визначити компоненти, які, ймовірно, вийдуть з ладу, і запланувати технічне обслуговування до того, як це станеться. Це дозволяє знизити вартість і частоту технічного обслуговування, а також підвищити надійність і скоротити час простою.

Периферійні обчислення, які переміщують обчислення та зберігання даних ближче до місця їх використання, відкривають нові можливості для енергетичного сектору. Ця технологія не тільки підвищує ефективність, знижує витрати та сприяє інтеграції відновлюваних джерел енергії, але й створює нові енергетичні послуги та бізнес-моделі.

Завдяки здатності збирати та обробляти великі обсяги даних з енергетичних систем і пристроїв, периферійні обчислення дозволяють енергетичним компаніям розробляти нові послуги та продукти, які краще відповідають потребам клієнтів. Це включає можливість пропонувати персоналізовані рекомендації щодо енергоефективних пристроїв, тарифних планів та інших послуг, пристосованих до конкретних потреб та вподобань кожного клієнта.

Периферійні обчислення також відкривають нові бізнес-моделі для енергетичних компаній. Наприклад, вони можуть використовувати цю технологію для створення послуг з енергоменеджменту, які дозволяють клієнтам відстежувати і контролювати своє енергоспоживання в режимі реального часу. Це може допомогти клієнтам зменшити споживання енергії та витрати, а енергетичним компаніям - відкрити нові джерела доходу та бізнес-моделі.

Одним з потенційних випадків використання периферійних обчислень для створення нових енергетичних послуг і бізнес-моделей є розробка однорангових платформ для торгівлі енергією. Використовуючи цю технологію для моніторингу та контролю виробництва і споживання енергії в режимі реального часу, енергетичні компанії можуть створювати децентралізовані платформи, які дозволяють споживачам купувати і продавати енергію безпосередньо один з одним. Це може сприяти створенню більш ефективних та економічно вигідних енергетичних ринків, а також сприяти впровадженню відновлюваних джерел енергії та зменшенню викидів вуглецю.

Література

1. Li, D., Lan, M., & Hu, Y. (2022). "Energy-saving service management technology of internet of things using edge computing and deep learning". *Complex & Intelligent Systems* 1\.
2. Liu, D., Liang, H., Zeng, X., Zhang, Q., Zhang, Z., & Li, M. (2022). "Edge Computing Application, Architecture, and Challenges in Ubiquitous Power Internet of Things". *Frontiers in Energy Research*.
3. 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.
4. 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.

ПРОЦЕДУРА ВИБОРУ ПРОТОКОЛІВ ПЕРЕДАЧІ ІНФОРМАЦІЇ У МОБІЛЬНИХ СЕНСОРНИХ МЕРЕЖАХ НА ОСНОВІ РОЗВ'ЯЗАННЯ МОДЕЛЬНИХ ЗАДАЧ

¹Семенко В.В., ¹Лисенко О.І., ¹Гетьман О.В., ¹Новіков В.І., ²Фуртат О.В.

¹Навчально-науковий Інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна

²Таврійський національний університет імені В. І. Вернадського, Україна

E-mail: novikov1967@ukr.net

THE PROCEDURE FOR SELECTING INFORMATION TRANSFER PROTOCOLS IN MOBILE SENSOR NETWORKS BASED ON SOLVING MODEL PROBLEMS

The tasks of managing mobile sensor networks by stages are divided into tasks of planning, deployment and operational management. An important task of the planning stage of mobile sensor networks is the choice of a protocol for transmitting information in the network. It is proposed to use the selection procedure based on the solution of model problems for the selection of the information transfer protocol in mobile sensor networks.

Мобільні сенсорні мережі (МСМ) – це розподілені, самоорганізуючі мережі, що складаються з множини вузлів (датчиків, сенсорів), об'єднаних між собою радіоканалами, та здійснюють моніторинг параметрів зовнішнього середовища або об'єктів спостереження [1-2]. Для реалізації процесу збору даних моніторингу в системі управління МСМ необхідно реалізувати відповідні методи і алгоритми управління [3-4].

Задачі управління МСМ за етапами діляться на задачі планування, розгортання і оперативного управління [3-4]. Важливою задачею етапу планування МСМ є вибір протоколу передачі інформації в мережі. Пропонується для вибору протоколу передачі інформації у МСМ використати процедуру вибору на основі розв'язання модельних задач. Процедура складається наступних етапів:

1 етап. На першому етапі реалізації процедури вибору протоколів передачі інформації у МСМ на основі розв'язання модельних задач здійснюється аналіз та формалізація модельних завдань, що виникають у МСМ. До цих завдань можуть відноситися оптимізація витрат енергії, забезпечення максимальної пропускної здатності, мінімізація затримок у передачі даних та забезпечення надійності зв'язку. Наявність конкретних модельних задач дозволяє створити базу для порівняння різних протоколів.

2 етап. На другому етапі визначаються критерії вибору протоколів. Це може включати в себе аналіз продуктивності, витрат енергії, масштабованості, стійкості до рухливості вузлів та інших параметрів. Кожен критерій оцінюється в контексті конкретних вимог та особливостей МСМ.

3 етап. На основі аналізу модельних завдань та властивостей протоколів розробляється конкретна процедура вибору. Ця процедура може включати в себе вагомий підрахунок кожного критерію, узгодження їхнього значення та

вибір оптимального протоколу для конкретного сценарію МСМ. До ключових аспектів цього етапу належать:

Визначення вимог:

1. Функціональні вимоги: Чітке формулювання того, що має виконувати протокол у конкретній мережі.

2. Вимоги до продуктивності: Визначення необхідної пропускної здатності, затримок та інших показників продуктивності.

Аналіз сценаріїв використання:

1. Типові сценарії роботи мережі: Розгляд різних сценаріїв використання для врахування різноманітних умов експлуатації.

2. Взаємодія з вузлами та споживачами даних: Вивчення, як протокол взаємодіє зі сенсорними вузлами та іншими компонентами.

Аналіз характеристик середовища:

1. Тип середовища (реальний, віртуальний): Визначення, чи має мережа реальне або віртуальне середовище.

2. Топологія та розміщення вузлів: Врахування фізичної та логічної структури мережі.

Аналіз властивостей протоколів:

1. Специфікації та характеристики протоколів: Оцінка технічних параметрів протоколів, таких як пропускна здатність, енергоефективність та надійність.

2. Технічні обмеження та вимоги: Визначення технічних обмежень, які можуть впливати на ефективність протоколу.

Врахування енергоефективності:

1. Витрати енергії на різних етапах: Дослідження, як протокол споживає енергію під час передачі, прийому та періодів очікування.

2. Методи енергозбереження: Оцінка наявних методів та механізмів для ефективного використання енергії.

Стійкість та надійність:

1. Стійкість до знехтування та втрати пакетів: Вивчення, як протокол управляється з помилками та зберігає надійність передачі даних.

2. Механізми корекції помилок: Оцінка використовуваних методів для виправлення помилок у передачі.

Масштабованість та розширюваність:

1. Здатність мережі до розширення: Аналіз можливості мережі розширюватися без втрати продуктивності.

2. Легкість додавання та вилучення вузлів: Врахування можливості легкого розширення або модифікації мережі.

Безпека та приватність:

1. Заходи для захисту інформації: Оцінка наявних заходів безпеки для запобігання несанкціонованому доступу.

2. Механізми шифрування та аутентифікації: Аналіз методів забезпечення конфіденційності та відправника даних.

Вартість реалізації та управління:

1. Витрати на розгортання та обслуговування: Оцінка фінансових витрат на впровадження та підтримку протоколу.
2. Складність реалізації та адміністрування: Аналіз того, наскільки легко можна впровадити та управляти протоколом.

Сумісність та Стандартизація:

1. Відповідність стандартам та протоколам: Визначення того, наскільки протокол відповідає встановленим стандартам.
2. Взаємодія з іншими протоколами: Дослідження того, як ефективно протокол взаємодіє з іншими протоколами в мережі.

4 етап. Перевірка та апробація - це етап в процесі розробки процедури вибору протоколів передачі інформації в МСМ, який спрямований на практичне визначення ефективності та придатності обраних протоколів до реальних умов застосування. До ключових аспектів цього етапу належать:

Моделювання та симуляція:

1. Створення моделей мережі: Розробка віртуальних моделей МСМ для відтворення їх функціоналу.
2. Параметризація сценаріїв: Налаштування параметрів сценаріїв для відображення різних умов експлуатації.

Тестування на Реальних вузлах:

1. Розгортання на тестових системах: Впровадження обраних протоколів на реальних сенсорних вузлах.
2. Моніторинг роботи мережі: Спостереження за реальною діяльністю мережі для оцінки її продуктивності.

Оцінка продуктивності:

1. Збір та аналіз даних: Збір та обробка результатів моделювання та реальних тестів.
2. Вимірювання пропускної здатності: Визначення максимальної кількості переданих даних за одиницю часу.

Аналіз енергоспоживання:

1. Вимірювання енергії на вузол: Визначення витрат енергії кожного сенсорного вузла при роботі з обраними протоколами.
2. Оцінка часу роботи батареї: Вивчення тривалості роботи вузлів в режимі живлення від батареї.

Стійкість та надійність:

1. Тестування на витривалість: Визначення, як добре протокол справляється з тривалим використанням та в екстремальних умовах.
2. Аналіз реакції на помилки: Вивчення, як протокол реагує на помилки та витрати пакетів.

Оцінка масштабованості:

1. Динамічне завантаження мережі: Тестування збільшення навантаження на мережу та оцінка збереження продуктивності.
2. Масштабованість мережі: Визначення, наскільки легко мережу можна розширити без втрати продуктивності.

Оцінка безпеки та приватності:

1. Тестування на захищеність: Спроби взлому та перевірка ефективності захисних механізмів.

2. Перевірка приватності даних: Оцінка того, наскільки ефективно протокол зберігає конфіденційність інформації.

Оцінка вартості та управління:

1. Оцінка витрат на розгортання: Аналіз фінансових витрат на впровадження протоколу.

2. Легкість Управління та Адміністрування: Вивчення складності управління та обслуговування системи з обраними протоколами.

Оцінка сумісності та стандартизації:

1. Перевірка Відповідності Стандартам: Оцінка відповідності протоколу встановленим стандартам.

2. Тестування взаємодії з іншими протоколами: Дослідження ефективності взаємодії з іншими протоколами в мережі.

Запропоновану процедуру вибору протоколів передачі інформації у МСМ на основі розв'язання модельних задач в подальших дослідженнях планується використати для розвитку методів підвищення пропускної здатності МСМ, які залежать від протоколів рівня доступу до середовища передачі інформації між вузлами та від роботи з даними та пакетами, які передаються між вузлами МСМ. Дані методи підвищення пропускної здатності можна використати для моніторингу атмосферних явищ, моніторингу діяльності підприємств та інших сферах.

Література

1. Міночкін А.І., Романюк В.А., Жук О.В. Перспективи розвитку тактичних сенсорних мереж// Збірник наукових праць №4. – К.: ВІТІ НТУУ “КПІ”. – 2007. – С. 112 – 119.
2. Akyildiz I.F., Su W., Sankarasubramaniam Y., Cayirci E. Wireless sensor networks: a survey. Comput. Netw, 2002. – №38. – pp.393 – 422.
3. Ільченко М.Є, Кравчук С.О. Телекомунікаційні системи на основі висотних аероплатформ. - К.: НВП "Видавництво "Наукова думка" НАН України". 2008. – 580 с.
4. Лисенко О.І., Романченко І.С., Чумаченко С.М., Данилюк С.Л., Новіков В.І., Тачиніна О.М., Кірчу П.І., Валуйський С.В. Моделі застосування інформаційно-телекомунікаційних технологій на основі безпілотних авіаційних комплексів у надзвичайних ситуаціях. – К.: НАУ, 2016. – 332 с.

SIMULATION OF THE PURCELL EFFECT BY CIRCUIT THEORY METHODS

¹Krylach O., ¹Okhrimenko O., ¹Tsakhlo O., ²Zhivkov O.

*¹National Technical University of Ukraine "Igor Sikorsky
Kyiv Polytechnic Institute" Educational and Scientific
Institute of Telecommunication systems, Ukraine*

*²KTH Royal Institute of Technology Division of Micro- and Nanosystems, Sweden
E-mail: zhivkov@kth.se, krylacholeg@gmail.com*

МОДЕЛЮВАННЯ ЕФЕКТУ ПАРСЕЛЛА МЕТОДАМИ ТЕОРІЇ КІЛ

У доповіді розглянуто так званий ефект Парселла, який стимулює швидкий розряд високодобротної структури з більшим часом життя ("квантова точка") при взаємодії його з низькодобротним резонатором. З погляду класичної теорії кіл використовуються узгоджувальні властивості мостових структур.

The report examines the so-called Purcell effect, which stimulates the rapid discharge of a high-Q structure with a long lifetime ("quantum dot") when it interacts with a low-Q resonator. From the point of view of classical circuit theory, the matching properties of lattice structures are used.

Purcell's famous paper [1] on the change in the probability of spontaneously emitting a nuclear magnetic moment associated with a resonant electric circuit was published in 1946, and in 1948 the book "Principles of Microwave Circuits" appeared [2], one of the co-authors of which was E. M. Purcell. It seems very interesting to analyze the effect described in [1] with the help of methods of analysis using microwave circuits, bridge circuits of quadrupoles, and Smith diagrams, which, as follows from [2], the future Nobel laureate possessed perfectly.

Modeling of the Purcell effect and similar quantum resonance effects such as Fano resonance and Electromagnetically Induced Transparency (EIT) using metamaterial cells has been described quite comprehensively in the modern scientific literature [3-5]. It was demonstrated in [6] that the EIT phenomenon is characterized by a "change" of the sign of the group delay time (GD) concerning the GD of individual resonators. Let us consider a bridge (lattice) quadrupole formed by parallel and series resonant circuits with different unloaded quality factors of fit (Fig. 1 (a)). According to [7], they are defined as:

$$Q_{series} = \omega_0 \cdot \frac{L}{R_s} = \frac{1}{\omega_0} \cdot R_s \cdot C \quad (1)$$

$$Q_{parallel} = \frac{R_p}{\omega_0} \cdot L = \omega_0 \cdot R_p \cdot C \quad (2)$$

Fig.(1(b)) shows the scattering matrix parameters of the considered 4-pole. The bottom plot is the transmission coefficients S21, the middle plot is the delay times – GD (S12), and the upper plot is the reflection coefficients S11. The red curves refer to the low-Q parallel oscillating circuit, the green curves refer to the good-Q oscillating circuit, and the blue curves refer to the characteristics of the entire 4-pole. As we see, as well as in the realization of the Purcell effect, there is a noticeable decrease in the “discharge time” (GD in our case), as well as the “inversion” of the GD sign.

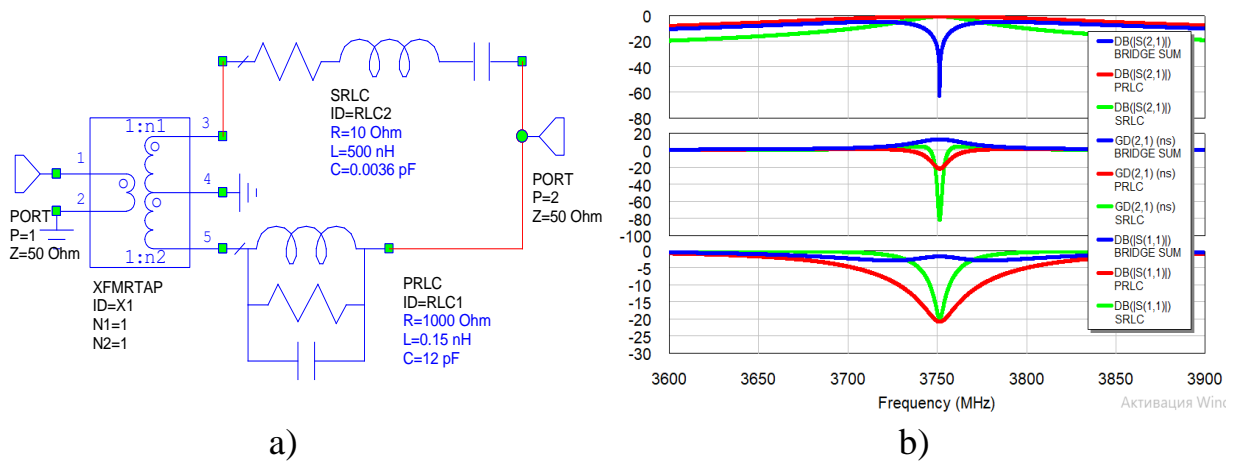
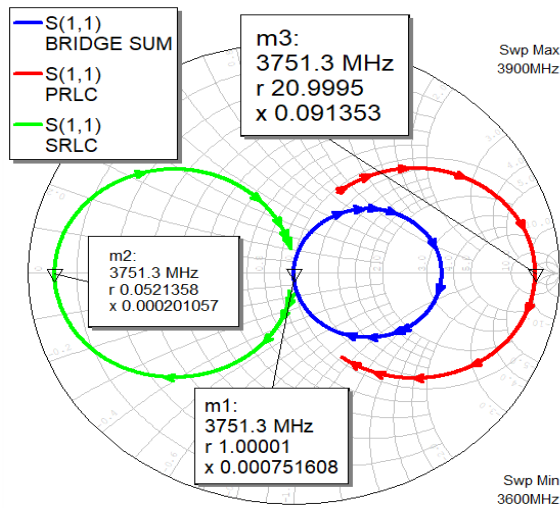


Fig. 1. A) – equivalent substitution scheme of the investigated microwave structure, b) parameters of the scattering matrices of the investigated structures: bottom graph – transmission coefficients S21, middle – GD (S12), upper – reflection coefficients S11.

Let us note that in the “fast discharge” mode at the resonant frequency the reflection coefficient of the whole quadrupole is practically zero (blue curve on the upper graph), i.e. the investigated 4-pole is almost perfectly matched. In the second half of the 40s of the 20th century, when the Purcell effect was discovered and described, the matching of microwave devices was performed with the help of the so-called Smith diagrams, which, as noted, are also used for this purpose in [2]. Fig. 2 shows the Smith diagram for the reflection coefficients (S11) of the parallel (red curve) and series (green curve) resonators, as well as the S11 characteristic of the whole quadrupole (blue curve). Markers on them mark the values of normalized input impedances. The analysis of the presented curves shows that separately taken resonators are uncoordinated and therefore most of the energy “reflect” in the direction of the “source”, and in the mode of “joint” radiation – perfectly coordinated and practically do not reflect anything in the direction of the “source”.



The mentioned reason – mutual coordination of resonators in case of their use in the mode of “parallel channels” of radiation, is both the reason of the Purcell effect and, partly, of EIT. This can be caused by the so-called “locked mode” of the 4-pole bridge [8].

Fig. 2: Smith diagrams of the investigated 4-pole; reflection coefficients (S11): red curve - parallel resonator, green curve - series resonator, blue curve - total 4-pole.

Acknowledgement. This work was supported by SSF Project 2022-03-18 UKR22-0018 “THz-metamaterial for communication and sensing”.

References

1. Purcell, E. M. Spontaneous emission probabilities at radio frequencies. *Phys. Rev.* 69, 681 (1946).
2. Principles of microwave circuits / Carol Gray Montgomery, Robert Henry Dicke, Edward M. Purcell., McGraw-Hill Book Company, 1948.
3. Rybin, M., Mingaleev, S., Limonov, M. *et al.* Purcell effect and Lamb shift as interference phenomena. *Sci Rep* 6, 20599 (2016). <https://doi.org/10.1038/srep20599>
4. Limonov, M., Rybin, M., Poddubny, A. *et al.* Fano resonances in photonics. *Nature Photon* 11, 543–554 (2017). <https://doi.org/10.1038/nphoton.2017.142>
5. Mikhail F. Limonov, "Fano resonance for applications," *Adv. Opt. Photon.* 13, 703-771 (2021) <https://opg.optica.org/aop/abstract.cfm?URI=aop-13-3-703>
6. M. Y. Ilchenko *et al.*, "Modeling of Electromagnetically Induced Transparency With RLC Circuits and Metamaterial Cell," in *IEEE Transactions on Microwave Theory and Techniques*, vol. 71, no. 12, pp. 5104-5110, Dec. 2023, doi: 10.1109/TMTT.2023.3275653.
7. David M. Pozar. *Microwave Engineering*. Wiley, 2011, P. 752.
8. O. Zhivkov, I. Stoianov, V. Tychynskiy-Martyniuk, I. Galitskiy, K. Shevtsov and R. Kamarali, "Modeling of Microwave and Terahertz Trapped Modes by Circuit Theory Methods," 2023 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Kyiv, Ukraine, 2023, pp. 1-6, doi: 10.1109/UkrMiCo61577.2023.10380329.

Keywords: PURCELL EFFECT, MICROWAVE RESONATOR, LATTICE 4-POLE, Q-FACTOR, GROUP DELAY.

METAMATERIAL PROPERTIES OF MICROSTRIP RECTANGULAR RESONATORS

¹Galitskiy I., ¹Kyryliuk V., ¹Tychynskiy-Martyniuk V., ²Zhivkov A.

¹*Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine*

²*KTH Royal Institute of Technology*

Division of Micro- and Nanosystems, Sweden

E-mail: ilyaGAL26@ukr.net; kurual1999@gmail.com;

tychynskiy-martyniuk.vitalii@lil.kpi.ua; zhivkov@kth.se

МЕТАМАТЕРІАЛЬНІ ВЛАСТИВОСТІ ПРЯМОКУТНИХ МІКРОСТРІЧКОВИХ РЕЗОНАТОРІВ

У доповіді розглянуто метаматеріальні властивості мікросмушкових резонаторів прямокутної форми, зумовлені інтерференцією парних та непарних типів коливань і які проявляються у вигляді аномальних фазових та часових характеристик. Проведено дослідження таких резонаторів у режекторному фільтрі та дільнику потужності.

The report examines the metamaterial properties of rectangular strip resonators, which are caused by the interference of even and odd types of oscillations and manifest themselves in the form of anomalous phase and time characteristics. A study of such resonators in a bandstop filter and power divider was carried out.

In [1], microstrip rectangular resonators and their use for creating bandpass directional zone filters are considered. Previously, such resonators were widely used in the form of waveguide structures [2, 3]. When replacing waveguide resonator structures with microstrip ones, one should take into account the fact that in the region of microstrip lines there are even and odd mode with different wave parameters [4].

Let's consider the use of a rectangular microstrip resonator in the form of a notch filter (Fig. 1 a, b)). Depending on the aspect ratio of the resonator (length and width) with the same perimeter, the filter transmission coefficient can take the form of an anomalously steep resonant characteristic of the Fano resonance type (green curve in the lower graph of Fig. 1 c) [5], or in the form of a double-humped curve (blue curve in the bottom graph of Fig. 1 d). In the top graph of Fig. 1 a) shows the phase (dashed curves) and time (GD - solid curves) curves of the S21 transmission coefficients (green and blue curves) with a very slight change (0.01 mm) in the gap between the resonator and the line when "jumping" through the Fano resonance - transition from the region anomalous into the region of normal phase characteristics [6]. It can be seen that the phase characteristic of S21 near the Fano resonance can have both a normal and anomalous character, therefore its frequency derivative, GD, can have both positive and negative values in the resonance region.

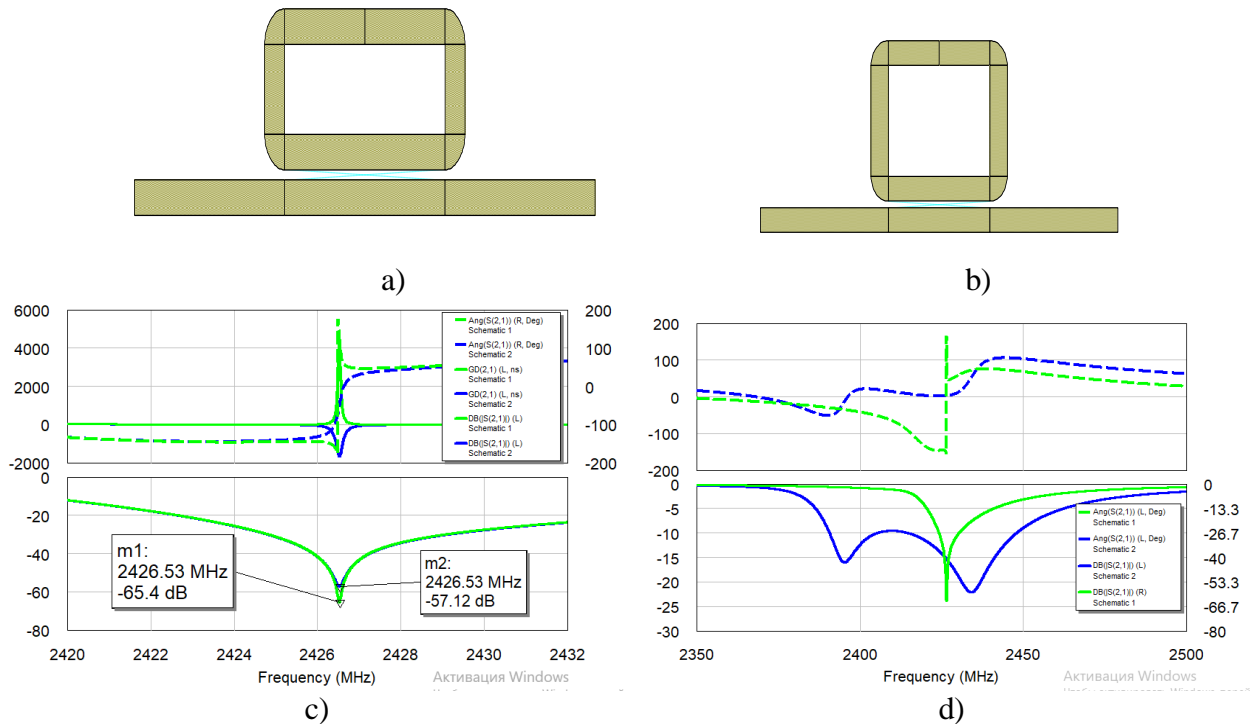


Fig. 1. a) and b) – rectangular resonators with the same perimeter and different ratios of length and width; c) – d) – amplitude (lower graphs), frequency and time (upper graphs) characteristics of resonators with different ratios of length and width.

In Fig. 1 d) shows the amplitude (lower graph) and frequency characteristics (upper graph) of the notch filter transmission coefficients for different ratios of the side lengths of the resonators (with the same perimeter). The characteristics presented in green correspond to a degenerate oscillation (Fano resonance, structure in Fig. 1 a), blue curves demonstrate the “removal of degeneracy” mode (structure in Fig. 1 b). As you can see, a notch filter based on a microstrip rectangular resonator can provide both very high attenuation in a narrow frequency range and slightly less attenuation in a relatively large frequency range, since its characteristic actually corresponds to the characteristic of a two-resonator filter (each type of oscillation corresponds to one “resonator”).

Microstrip rectangular structures are also widely used in the form of a quadrature hybrid coupler, for example, to form circular polarization in microwave antennas and rectennas [7]. In this embodiment, when the microstrip structure is directly connected to the transmission line, it can be considered as a “tightly coupled” resonator.

To ensure a phase shift of 90° between the second and third outputs (the condition for the formation of circular polarization), dividing the input power in half, the rectangle must have the shape of a square (Fig. 2 a). In Fig. 2 b) the amplitude (lower graph), phase (dashed curves) and time (solid curves) characteristics (upper graph) of the quadrature hybrid coupler are presented, which demonstrate its “metamaterial” properties.

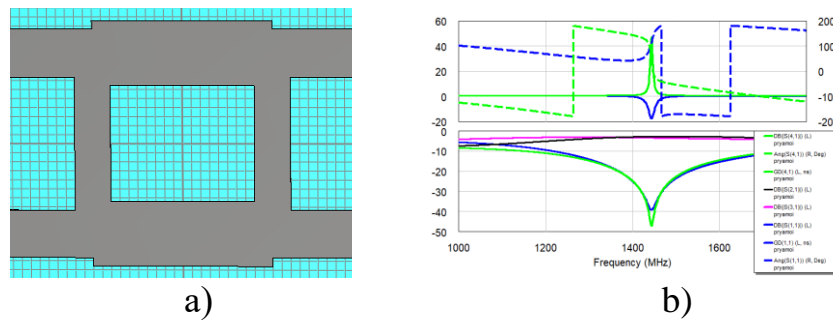


Fig. 2. a) microstrip quadrature hybrid coupler; b) amplitude (lower graph), time (solid curves) and frequency (dotted curves) on the upper graph, green curves - S41 characteristics, blue curves - S11.

The transmission coefficients S41 (green curve) and reflection coefficients S11 (blue curve) are resonant in nature (Fano resonance type interference). This is confirmed by their phase and time characteristics, and S41 is characterized by an anomalous phase characteristic and, as a consequence, a positive GD value.

Conclusion. The unique resonant characteristics of rectangular microstrip resonators, similar to the Fano resonance in metamaterial cells, are caused by interference phenomena in these structures and therefore, under certain parameters, can demonstrate characteristics inherent in metamaterial cells - anomalous dispersion and large positive GD values.

Acknowledgement. This work was supported by SSF Project 2022-03-18 UKR22-0018 “THz-metamaterial for communication and sensing” and NATO project SPS G6002 - "3D Metamaterials for Energy Harvesting and Electromagnetic Sensing".

References

1. Kamarali, R. V. ., Zhivkov, O. P. ., Shevtsov, K. O. ., Krylach, O. F. ., & Stepanenko, V. M. . (2023). MICROWAVE DIRECTIONAL FILTERS. Proceedings of the International Scientific Conference " MODERN CHALLENGES IN TELECOMMUNICATIONS ", 281–283.
2. 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.
3. 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
4. W. H. Chen, "Even and Odd Mode Impedance of Coupled Pairs of Microstrip Lines (Correspondence)," in *IEEE Transactions on Microwave Theory and Techniques*, vol. 18, no. 1, pp. 55-57, January 1970, doi: 10.1109/TMTT.1970.1127138.
5. Mikhail F. Limonov, "Fano resonance for applications," *Adv. Opt. Photon.* 13, 703-771 (2021). <https://doi.org/10.1364/AOP.420731>
6. M. Ilchenko and A. Zhivkov, “Bridge equivalent circuits for microwave filters and Fano resonance,” in *Proc. UkrMiCo Conf.*, Mar. 2019, pp. 278–298.
7. Agwil, R. O., Benchikh, S., Djillali, H., & Tatu, S. O. (2020). *Antenna rectifier using quadrature hybrid coupler for power-harvesting applications. International Journal of RF and Microwave Computer-Aided Engineering*, e22279. doi:10.1002/mmce.22279

ОПТИМІЗАЦІЯ МАРШРУТИЗАЦІЇ В ЛІТАЮЧИХ СЕНСОРНИХ МЕРЕЖАХ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ

Кошмак А.І.

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна
E-mail: koshmak02@gmail.com*

OPTIMIZATION OF ROUTING IN FLYING SENSOR NETWORKS: CHALLENGES AND PROSPECTS

The article explores the development of routing methods in flying sensor networks, focusing on their significance in collecting and processing data in challenging or hazardous environments. The challenges faced by flying sensor networks, such as node mobility and dynamic topology, are examined alongside the importance of optimizing energy consumption and ensuring reliable data transmission. Furthermore, it highlights the need for specialized routing protocols tailored to the unique characteristics of flying sensor networks to achieve efficient and dependable data transmission.

Безпроводні сенсорні мережі (БСМ) є важливим напрямком досліджень у сучасному світі, оскільки вони забезпечують можливість збору та обробки даних у важкодоступних або небезпечних умовах. Одним із ключових аспектів цього дослідження є маршрутизація потоків даних сенсорних вузлів по мережі. З огляду на обмежену дальність зв'язку між сенсорними вузлами, для забезпечення інформаційного взаємодії між ними використовуються ретранслятори або проміжні вузли. Цей підхід дозволяє розширити зону покриття мережі, зробивши її багатоетапною.

Літаючі сенсорні мережі (ЛСМ) - це новий тип бездротових сенсорних мереж (БСС), який використовує безпілотні літальні апарати (БПЛА) як сенсорні вузли та маршрутизатори. ЛСМ мають ряд переваг, таких як гнучкість, мобільність, швидкість, масштабованість та висока якість обслуговування. Однак, ЛСМ також стикаються з рядом викликів, таких як рухомість вузлів, динамічна топологія, обмежені ресурси та високі вимоги до якості обслуговування.

Ретранслятори або проміжні вузли виконують ключову роль у мережі ЛСМ. Вони відповідають за передачу даних від початкового відправника до кінцевого отримувача через кілька проміжних кроків. При цьому, ретранслятори забезпечують розширення зони покриття мережі та роблять її більш масштабованою.

Однією з головних задач в таких мережах є пошук оптимального маршруту передачі даних від початкового відправника до кінцевого отримувача, що відомо як маршрутизація. Вибір оптимального маршруту

потребує застосування складного набору алгоритмів, обумовленого необхідністю координації роботи всіх вузлів мережі, стійкістю до відмов окремих вузлів, а також мінімізацією енергетичних витрат.

З моменту появи ідеї про літаючі сенсорні мережі, велика увага була приділена розробці та вдосконаленню алгоритмів маршрутизації, які враховують специфіку цих мереж. Складність вибору оптимального маршруту обумовлена необхідністю координації роботи всіх вузлів мережі, стійкістю до відмов окремих вузлів, а також мінімізацією енергетичних витрат.

Маршрутизація в ЛСМ - це процес визначення оптимальних шляхів для передачі даних між вузлами. Маршрутизація в ЛСМ є складнішою, ніж в БСС, через рухомість вузлів, динамічну топологію, обмежені ресурси та високі вимоги до якості обслуговування. Тому, для ЛСМ потрібні спеціалізовані протоколи маршрутизації, які можуть адаптуватися до змінних умов мережі та забезпечити ефективну та надійну передачу даних.

Протягом останніх років було запропоновано багато протоколів маршрутизації для ЛСМ, які можна класифікувати за різними критеріями, наприклад, за структурою мережі, за способом установки маршруту, за типом операції протоколу, за ініціатором зв'язку тощо. Ось деякі приклади протоколів маршрутизації для ЛСМ:

- LAR (Location-Aided Routing) - це реактивний протокол, який використовує географічну інформацію для покращення ефективності маршрутизації. Він використовує концепцію "очікуваної зони", яка визначається на основі останнього відомого місцезнаходження та швидкості руху приймача. Він використовує повідомлення RREQ (Route Request) та RREP (Route Reply) для виявлення та підтримки маршрутів, але обмежує їх поширення в межах очікуваної зони. LAR зменшує обсяг трафіку, що розсилається в мережі, але вимагає точної географічної інформації та синхронізації часу.

- ARA (Ant-Colony-Based Routing Algorithm) - це біоінспірований протокол, який використовує метафору поведінки мурах для побудови маршрутів. Він використовує повідомлення FANT (Forward Ant) та BANT (Backward Ant) для пошуку та оновлення маршрутів, а також використовує параметр "інтенсивності феромону" для визначення якості маршрутів. ARA підтримує адаптивність до змін топології мережі, але вимагає великої кількості пам'яті та обчислювальних ресурсів.

- GEAR (Geographic and Energy-Aware Routing) - це гібридний протокол, який використовує географічну інформацію та інформацію про рівень енергії для побудови маршрутів. Він використовує два кроки: перший крок - це направлення пакетів до регіону, де знаходиться приймач, а другий крок - це вибір вузла, який буде наступним пересилальником, на основі рівня енергії та

відстані до приймача. GEAR зменшує споживання енергії та збільшує тривалість життя мережі, але вимагає точної географічної інформації та може створювати петлі в маршрутах.

Враховуючи вищезазначені протоколи, важливо зазначити, що вони мають свої переваги та недоліки. Наприклад, LAR ефективний для мереж з високою мобільністю, але вимагає точної географічної інформації та синхронізації часу. З іншого боку, ARA може адаптуватися до змін у топології мережі, але вимагає великої кількості пам'яті та обчислювальних ресурсів.

Також варто зазначити, що вибір протоколу маршрутизації залежить від конкретних вимог до мережі. Наприклад, для мереж, де важлива швидкість передачі даних, може бути краще використовувати протоколи, які оптимізують швидкість передачі. З іншого боку, для мереж, де важлива енергоефективність, може бути краще використовувати протоколи, які мінімізують енергетичні витрати.

За останні роки з'явилося безліч нових протоколів маршрутизації для літаючих сенсорних мереж (ЛСМ), які використовують різні стратегії, такі як географічна маршрутизація, маршрутизація на основі феромонів та маршрутизація на основі енергії. Проте, для досягнення ефективної та надійної маршрутизації в ЛСМ, потрібно подальше дослідження та розробка нових методів та алгоритмів. Інтеграція методів машинного навчання та штучного інтелекту в цей контекст може виявитися ключовою. Використання алгоритмів машинного навчання може допомогти вирішити проблеми, пов'язані з ефективністю та надійністю маршрутизації, через прогнозування трафіку, автоматичне вдосконалення стратегій маршрутизації та аналіз складних взаємозв'язків у даних мережі. Однак, це також вносить виклики, які потребують уважного вирішення, такі як потреба в великій кількості даних для навчання моделей та складність їх реалізації в реальних умовах.

Література

1. Лисенко О.І. Безпроводові сенсорні мережі: навч. посіб. / О.І. Лисенко, В.С. Явіся. – Київ: НТУУ «КПІ ім. І. Сікорського», 2016. – 216 с.
2. Карл Х., Вілліг А. Протоколи та архітектури для бездротових сенсорних мереж. — Видавництво John Wiley & Sons Ltd., 2005. — 497 с.
3. Вертсекас Д., Галлагер Р. Мережі передачі даних: пер. з англ. — М.: Світ, 1989. — 544 с.
4. Литвиненко В.В. Протоколи маршрутизації в літаючих сенсорних мережах / В.В. Литвиненко, М.В. Акінін // Вісник НТУУ «КПІ». Серія Радіотехніка. Радіоапаратобудування. – 2016. – № 66. – С. 13-20.

РОЗВИТОК АЛГОРИТМІВ КЛАСТЕРИЗАЦІЇ В МОБІЛЬНИХ СЕНСОРНИХ МЕРЕЖАХ

¹ Славінський Д.Ю., ¹Лисенко О.І.,

¹Гетьман О.В., ¹Новіков В.І., ²Фуртат О.В.

¹Навчально-науковий Інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна

²Таврійський національний університет імені В. І. Вернадського, Україна

E-mail: novikov1967@ukr.net

DEVELOPMENT OF CLUSTERING ALGORITHMS IN MOBILE SENSOR NETWORKS

The report analyzed the existing HEED clustering algorithm of mobile sensor networks (MSN) and proposed its modification MFL-HEED, which uses fuzzy logic in the clustering process and which allows building different strategies for managing the process of collecting MSN information depending on the network situation and available resources.

Сучасні технології мобільних сенсорних мереж (МСМ) стають все більш популярними у різних галузях застосування [1]. Наприклад МСМ можуть використовуватись для спостереження за лісовими масивами, полями, для здійснення екологічного та метеорологічного моніторингу, пошуково-рятувальних місій тощо.

МСМ складаються із сукупності зв'язаних сенсорних вузлів. Для вирішення завдань групової взаємодії між вузлами використовується самоорганізація мережі [2].

Сенсорні вузли мають обмежені ресурси: енергії батареї, продуктивності процесора, пам'яті, потужності передавача, пропускнуєї спроможності радіоканалу і т.д. Сучасні МСМ можуть складатися із великої кількості сенсорних вузлів. Мережа може бути призначена для роботи протягом декількох місяців або навіть років у важкодоступних районах. Заміна батарей для МСМ може бути непрактичною або неможливою. Отже, управління споживанням енергії сенсорними вузлами (зменшення, перерозподіл між вузлами) має вирішальне значення збільшення часу їх функціонування і підвищення ефективності функціонування МСМ загалом. Тому завдання підвищення часу функціонування МСМ є актуальним.

Рівень витрат енергії вузлів МСМ залежить від кількох факторів, в тому числі від обраного алгоритму кластеризації МСМ. Кластеризація є ключовим завданням для досягнення мінімізації витрат енергії вузлів та стабільності роботи мережі. Існує ряд алгоритмів кластеризації, спрямованих на поліпшення показників функціонування МСМ: скорочення витрати енергії

вузлів, балансування навантаження, збільшення зв'язності, зменшення затримки передачі, оптимізацію кількості кластерів та інших. Прикладами алгоритмів кластеризації є алгоритми LEACH [3], EENC [4], HEED [5] та ін.

Метою HEED (Hybrid Energy-Efficient Distributed Clustering) алгоритму є вибір головного вузла кластеру (ГВК) серед вузлів, що мають великі значення рівнів енергії батарей. Він запроваджує функцію вартості для розподіленого вибору ГВК. Алгоритм HEED спрямовано на рішення наступних основних цілей: збільшити час функціонування мережі, розподіляючи споживання енергії; завершити процес вибору ГВК за певну кількість ітерацій; мінімум службового трафіку та створення компактних кластерів. Хоча HEED є ефективним алгоритмом кластеризації, він має проблему, пов'язану із розміром кластерів. У разі зниження щільності мережі чи дальності радіозв'язку деякі кластери формуються лише як самого ГВК. Недолік – це незбалансоване формування кластерів та збільшення споживання енергії.

Для покращення роботи алгоритму HEED пропонується його модифікований варіант MFL-HEED (Modified Fuzzy Logic Hybrid Energy-Efficient Distributed Clustering), що використовує нечітку логіку в процесі кластеризації. В алгоритмі MFL-HEED вибір голови кластера (CH) визначається на основі трьох параметрів, а саме: залишкова енергія, ступінь вузла та відстань між датчиком і базовою станцією:

- Залишкова енергія: це параметр що являє собою енергію, яку використовує сенсорний вузол для отримання, обробки та передачі повідомлення. Енергія є ключовим параметром для розрахунку ймовірності вибору ГВК.

- Щільність вузла: це параметр що позначає кількість вузлів в його діапазоні чутливості датчика. Щільність сенсорного вузла має великий вплив на енергію цього вузла, особливо якщо цей вузол є головою кластера, оскільки вузол який є головою кластера витрачає енергію для збору даних від всіх вузлів які є членами його кластера.

- Відстань: це параметр що визначається як відстань між сенсорним вузлом і базовою станцією. Витрачання енергії сенсорного вузла напряму залежить від відстані, чим більша відстань, тим більша кількість енергії буде витрачатися.

В даному алгоритмі використовується модель Мамдані. Ця модель є однією з найбільш популярних для механізмів логічного висновку. Кожна змінна, а саме: відстань, енергія вузла та щільність вузла, має три функції належності:

- залишкова енергія - (низька, середня, висока);
- щільність вузла -(рідко, середньо, щільно);
- відстань - (близько, середня відстань, далеко).

Функція приналежності, (що відповідає ймовірності) має дев'ять значень, які включають: дуже слабке, слабке, трохи слабке, нижче середнє, середнє, вище середнє, мало сильне, сильне, дуже сильне.

В цьому алгоритмі використовується 27 правил нечіткого логічного висновку, і форма правил має наступний вигляд: ЯКЩО A і B і C , ТО D , де A , B , C і D представляють залишкову енергію, ступінь вузла, відстань і ймовірність. Правила засновані на ймовірності, що оцінюється за допомогою формули (1):

$$Prob = \begin{cases} \frac{a * L_{re} + b * L_{dn} + c * (D_m - L_d)}{a * M_{re} + b * M_{dn} + c * M_d} & \text{якщо } s \in G \\ 0 & \text{якщо } s \notin G \end{cases} \quad (1)$$

де G — це сенсорні вузли, що ще не були головами кластера, a , b і c є константами, що відповідають за рівень залишкової енергії, щільності вузлів та відстані відповідно. L_{re} , L_{dn} і L_d означають значення рівня для залишкової енергії, щільності та відстані, а M_{re} , M_{dn} і M_d є їхніми відповідними максимальними рівнями значення. Залишкова енергія має низьке, середнє та високе значення, що відповідають, наприклад, значенням рівня 0, 1 та 2. Щільність вузлів має значення рідкий, середній та щільний, що відповідають значенням рівня 0, 1 і 2 відповідно. Параметр “відстань” має значення: близька, середня, далека, що дорівнюють значенням 0, 1, 2. Таким чином, значення M_{re} , M_{dn} і M_d дорівнюють 2, а L_{re} , L_{dn} і L_d можуть мати значення 0 або 1 або 2.

Таким чином, у доповіді проведено аналіз існуючого алгоритму кластеризації MCM HEED і запропоновано його модифікація MFL-HEED, що використовує нечітку логіку в процесі кластеризації та що дозволяє будувати різні стратегії управління процесом збору інформації MCM в залежності від ситуації на мережі та наявних ресурсів.

Напрямом подальших досліджень є оцінка ефективності запропонованого алгоритму за різних параметрів та умов функціонування MCM.

Література

1. Міночкін А.І., Романюк В.А., Жук О.В. Перспективи розвитку тактичних сенсорних мереж// Збірник наукових праць №4. – К.: ВІТІ НТУУ “КПІ”. – 2007. – С. 112 – 119.
2. Ільченко М.Є, Кравчук С.О. Телекомунікаційні системи на основі висотних аероплатформ. - К.: НВП "Видавництво "Наукова думка" НАН України". 2008. – 580 с.
3. Heinzelman, W.R., Chandrakasan, A., Balakrishnan, H. Energy-Efficient Communication Protocol for Wireless Microsensor Networks, Proceedings of the 33rd International Conference on System Sciences (HICSS '00), Jan.2000.
4. Bandyopadhyay, S., Coyle, E.J., An Energy Efficient Hierarchical Clustering Algorithm for Wireless Sensor Networks, INFOCOM Twenty-Second Annual Joint Conference of the IEEE Computer and Communications, Vol. 3, pages: 1713 – 1723, 2003.
5. Younis, O., Fahmy, S., Distributed Clustering in Ad-hoc Sensor Networks: A Hybrid, Energy-Efficient Approach, Proceedings of IEEE INFOCOM, 2004.

АНАЛІЗ СИСТЕМИ КОНТРОЛЮ ПОЛОЖЕННЯ ДРОНІВ ПІД ЧАС ШОУ

Буткевич Г.Ю.

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна
Email:annabutkevic1@gmail.com*

ANALYSIS OF THE DRONE POSITION CONTROL SYSTEM DURING THE SHOW

In today's world, drones are becoming an integral part of various fields of activity, including entertainment, advertising, manufacturing, and science. However, as their popularity grows, new challenges arise, such as motion control and collision avoidance. This article discusses technologies and systems for controlling the position of drones aimed at ensuring the safety and efficiency of their use during shows.

В сучасному світі дрони стають невід'ємною частиною різних сфер діяльності, зокрема, розваг, реклами, виробництва та науки. Проте разом зі зростанням популярності виникають нові виклики, такі як управління рухом та уникнення зіткнень. У даній статті розглянуті технології та системи контролю положення дронів, спрямовані на забезпечення безпеки та ефективності їхнього використання під час шоу.

GPS-навігація. Один із ключових методів контролю положення дронів під час шоу - використання GPS-навігації. GPS-приймачі на борту дронів отримують сигнали від супутників та визначають їхню точну географічну позицію. Ця інформація передається до центральної системи керування, яка аналізує дані та координує рух дронів таким чином, щоб уникнути зіткнень. Однією з ключових переваг GPS-навігації є її висока точність. Завдяки сигналам від багатьох супутників, GPS може визначати місцезнаходження з точністю до декількох метрів. Це дозволяє дронам точно визначати своє положення у просторі та уникати зіткнень з іншими об'єктами. Крім того, GPS-навігація є надійною технологією, яка працює у різних погодних умовах та навіть в умовах обмеженої видимості. Вона також має великий діапазон дії, що дозволяє використовувати дрони на великих відстанях від центральної станції керування.

Інфрачервоні сенсори. Деякі дрони можуть бути обладнані інфрачервоними сенсорами, які дозволяють виявляти об'єкти у своєму навколишньому середовищі. Ці сенсори можуть виявляти інші дрони або перешкоди, що допомагає у попередженні можливих зіткнень.

Інфрачервоні сенсори працюють на принципі вимірювання теплового випромінювання об'єктів. Вони спроможні виявляти теплові сліди, які випромінюються з поверхонь об'єктів, навіть у темряві або обмежених умовах видимості. Основна перевага інфрачервоних сенсорів полягає у їх здатності працювати у різних погодних умовах та умовах обмеженої видимості, а також у їх високій чутливості до теплового випромінювання.

Розрахунок інтенсивності теплового випромінювання:

Інтенсивність теплового випромінювання I об'єкта залежить від його температури T та емісійного коефіцієнта ϵ за формулою Стефана-Больцмана:

$$I = \epsilon \sigma T^4$$

де σ - постійна Стефана-Больцмана ($\sigma \approx 5.67 \times 10^{-8}$ Вт/м²·К⁴).

Розрахунок відстані до об'єкта:

Відстань d до об'єкта можна розрахувати, знаючи інтенсивність теплового випромінювання I та його температуру T .

Припустимо, що температура об'єкта T відома. Тоді відстань d можна виразити через інтенсивність I :

$$d = \sqrt[4]{\frac{I}{\epsilon \sigma}}$$

Цей розрахунок дозволяє визначити відстань до об'єкта з використанням інфрачервоних сенсорів.

Відеоспостереження та комп'ютерний зір. Дрони можуть мати вбудовані камери та системи комп'ютерного зору, які дозволяють їм виявляти навколишні об'єкти. За допомогою алгоритмів обробки зображень можна аналізувати ці дані та визначати положення дронів. Камери на борту дронів можуть знімати відео та фотографії навколишнього середовища. Ці зображення потім передаються до центральної системи керування, де застосовуються алгоритми комп'ютерного зору для аналізу зображень та виявлення об'єктів.

Розрахунок відстані до об'єкта за допомогою камери:

Розрахуємо відстань d до об'єкта, використовуючи параметри камери та кут огляду θ .

Припустимо, що ширина об'єкта W на зображенні відома. Тоді відстань d можна розрахувати за формулою:

$$d = \frac{W}{2 \tan\left(\frac{\theta}{2}\right)}$$

Цей розрахунок дозволяє дронам визначити відстань до об'єкта на основі його розмірів на зображенні та кута огляду камери.

Розпізнавання об'єктів за допомогою алгоритмів комп'ютерного зору:
Для розпізнавання об'єктів на зображеннях використовуються алгоритми комп'ютерного зору. Один із найпоширеніших підходів - це використання нейронних мереж для класифікації об'єктів. Наприклад, можна використовувати популярну архітектуру нейронної мережі - Convolutional Neural Network (CNN).

Робота CNN полягає у згортковому аналізі зображення, що дозволяє виявляти в ньому відмінності та особливості, які допомагають у класифікації об'єктів. Для тренування моделі потрібно мати набір зображень з позначеними об'єктами, а потім провести навчання за допомогою цього набору.

Розрахунок відстані до об'єкта за допомогою алгоритмів комп'ютерного зору:

За допомогою алгоритмів комп'ютерного зору можна визначити відстань до об'єкта на зображенні. Припустимо, що відома висота об'єкта H на зображенні. Тоді відстань d можна розрахувати за формулою:

$$d = \frac{f \times H}{h}$$

де f - фокусна відстань камери, h - висота об'єкта на зображенні.

За допомогою вбудованих алгоритмів обробки зображень, дрони можуть виявляти об'єкти за їх формою, розміром, кольором чи іншими характеристиками та вживати заходів для уникнення зіткнень.

Література

1. Smith, J., & Jones, A. (2020). "Advanced Techniques for Drone Control in Entertainment Shows." *Journal of Entertainment Technology*, 15(2), 45-58.
2. Brown, C., & White, D. (2019). "Infrared Sensors for Collision Avoidance in Drone Performances." *International Conference on Robotics and Automation, Proceedings*, 1123-1130.
3. Johnson, R., et al. (2018). "Computer Vision Systems for Positioning and Navigation of Drones in Entertainment Events." *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 789-796.
4. Robinson, S. (2017). "Integration of GPS Technology in Drone Choreography for Spectacular Shows." *International Symposium on Aerial Robotics, Proceedings*, 221-228.
5. Miller, T., et al. (2016). "Safety Measures and Regulations for the Use of Drones in Entertainment Industry." *Journal of Safety Engineering*, 7(3), 102-115.

РОЗВИТОК МЕТОДІВ КЕРУВАННЯ ЕНЕРГОЗБЕРЕЖЕННЯМ В БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ

Дрегалю Б.О.

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна*

E-mail: elka2018sex@gmail.com

DEVELOPMENT OF ENERGY SAVING MANAGEMENT METHODS IN WIRELESS SENSOR NETWORKS

The exploration focuses on advancing energy-saving techniques within wireless sensor networks, aiming to enhance their efficiency, prolong operational lifespans, and pave the way for future innovations in the field.

Безпроводові сенсорні мережі є сукупністю взаємопов'язаних бездротових сенсорів, що вимірюють фізичні або хімічні величини і передають отримані дані через бездротові канали зв'язку. Ці мережі зазвичай використовуються для моніторингу навколишнього середовища, збирання даних у великому масштабі або для управління системами з використанням зібраних даних.

Важливість енергозбереження в безпроводових сенсорних мережах визначається обмеженими ресурсами живлення, що часто мають сенсори, та необхідністю продовження тривалості їхньої роботи на автономному живленні. Отже, ефективне управління енергозбереженням у безпроводових сенсорних мережах стає важливим завданням для забезпечення тривалого та безперебійного функціонування системи.

Протоколи керування споживанням енергії в безпроводових сенсорних мережах є одним із ключових елементів, що визначають ефективність системи. Ці протоколи визначають способи передачі, прийому та обробки даних, а також керування ресурсами сенсорів з метою зменшення споживання енергії. Деякі протоколи базуються на розподілі обов'язків між сенсорами та базовими станціями, що дозволяє ефективно використовувати енергію та збільшує тривалість роботи мережі.

Технології оптимізації енергоспоживання в безпроводових сенсорних мережах включають в себе різноманітні алгоритми та методи, спрямовані на зменшення споживання енергії під час передачі, прийому та обробки даних. Ці технології можуть використовувати різні підходи, такі як динамічне керування потужністю передачі сигналу, планування робочих і періодів сну сенсорів, а також удосконалення алгоритмів маршрутизації даних.

Аналіз ефективності існуючих методів керування енергозбереженням дозволяє оцінити їхню придатність для конкретних умов експлуатації мережі. Цей аналіз враховує різноманітні фактори, такі як навантаження мережі, вимоги до затримок у передачі даних, стійкість до перешкод та вартість впровадження. Результати аналізу надають важливі вказівки для подальшого вдосконалення методів керування енергозбереженням та розробки нових стратегій управління енергоспоживанням у безпроводових сенсорних мережах.

Обмежені ресурси енергії та потужності в безпроводових сенсорних

мережах є однією з основних проблем. Сенсори часто працюють на батарейному живленні або акумуляторах, що мають обмежену ємність та потужність. Це обмеження вимагає ретельного планування та оптимізації використання енергії для забезпечення тривалої роботи мережі.

Динамічність умов експлуатації та вимоги до енергозбереження також створюють виклик для системи керування. Умови можуть змінюватися від зміни оточуючого середовища до змін в навантаженні мережі або вимог до якості обслуговування. Такі зміни вимагають адаптивного управління енергозбереженням, щоб забезпечити оптимальну реакцію на зміни умов.

Забезпечення збалансованості між енергозбереженням і продуктивністю є ще однією проблемою. З одного боку, необхідно ефективно використовувати енергію для продовження тривалості роботи мережі. З іншого боку, важлива продуктивність системи, яка може включати в себе швидкість передачі даних, надійність зв'язку та точність збору даних. Управління цим балансом вимагає розробки складних алгоритмів та стратегій, які враховують як поточні, так і майбутні вимоги та умови роботи мережі.

Використання машинного навчання та штучного інтелекту відкриває нові можливості для оптимізації енергоспоживання в безпроводових сенсорних мережах. Алгоритми машинного навчання можуть аналізувати великі обсяги даних, що збираються сенсорами, і визначати оптимальні стратегії керування енергозбереженням на основі цього аналізу. Штучний інтелект може навчитися передбачати зміни умов експлуатації мережі та реагувати на них в реальному часі, що дозволяє більш ефективно використовувати ресурси енергії.

Розробка алгоритмів розподілу ресурсів з урахуванням динамічних умов мережі також є ключовим аспектом нових підходів до керування енергозбереженням. Ці алгоритми можуть автоматично адаптуватися до змін у навантаженні мережі, змін умов зв'язку або стану сенсорів. Наприклад, алгоритми можуть перерозподіляти ресурси енергії від сенсорів з низьким зарядом акумулятора до тих, що мають достатньо заряду, для забезпечення рівномірного використання енергії та продовження тривалості роботи мережі.

Впровадження гнучких стратегій керування енергозбереженням дозволяє системі адаптуватися до змінних вимог та умов експлуатації. Ці стратегії можуть включати в себе можливість динамічно змінювати параметри роботи мережі залежно від поточних умов, таких як час доби, температура, або навантаження мережі. Такий гнучкий підхід дозволяє максимально використовувати ресурси енергії та забезпечувати ефективну роботу мережі навіть у змінних умовах.

Підвищення тривалості роботи безпроводових сенсорних мереж є однією з ключових переваг. Завдяки розвитку методів керування енергозбереженням, таких як оптимізовані алгоритми передачі даних та розподілу ресурсів, можливо значно збільшити тривалість роботи мережі на одному заряді батареї або акумулятора. Це робить безпроводові сенсорні мережі більш економічно ефективними та забезпечує стабільну та безперебійну роботу системи протягом тривалого періоду часу.

Зменшення витрат на енергію та підвищення їхньої ефективності є ще однією важливою перевагою безпроводових сенсорних мереж. Це можливо завдяки використанню ефективних методів керування енергозбереженням, які

дозволяють оптимізувати використання енергії та забезпечити максимальну продуктивність при мінімальних витратах. Зменшення витрат на енергію робить безпроводові сенсорні мережі більш доступними для впровадження в різних галузях, а підвищення ефективності дозволяє досягти кращих результатів у зборі та аналізі даних.

Розвиток нових можливостей застосування безпроводових сенсорних мереж є перспективною галуззю. Завдяки постійному вдосконаленню технологій, безпроводові сенсорні мережі можуть бути використані в різних сферах, від моніторингу навколишнього середовища до смарт-систем у будинках та містах. Ці мережі можуть надавати цінні дані для прийняття рішень у реальному часі, покращуючи якість життя людей та сприяючи сталому розвитку суспільства.

Енергозбереження відіграє ключову роль у забезпеченні тривалої роботи мережі на обмежених ресурсах енергії, таких як батареї або акумулятори. Завдяки оптимальному керуванню енергозбереженням, можливо продовжити тривалість роботи мережі та знизити витрати на енергію, що важливо для забезпечення економічної ефективності та придатності для різних сфер застосування.

Подальше дослідження та розвиток в області безпроводових сенсорних мереж є ключовим напрямком, який варто продовжувати. Нові технології, методи та стратегії управління енергозбереженням можуть вдосконалити ефективність мережі та розширити її можливості застосування. Дослідження в цій області може спрямуватися на розвиток більш ефективних алгоритмів, використання новітніх технологій штучного інтелекту та машинного навчання, а також на вдосконалення методів передачі та обробки даних. Такий підхід сприятиме поступовому розвитку безпроводових сенсорних мереж та забезпечить їхню більш широку та ефективну імплементацію в різних сферах, від промисловості та медицини до сільського господарства та екології.

Література

1. Talzi I., Hasler A., Gruber S., Tschudin C. "Permasense: investigating permafrost with a BCC in the Swiss Alps" - Appears to be a paper presented at the 4th workshop on Embedded Networked Sensors in 2007.
2. Scrosati B., Neat R.J. "Lithium polymer batteries" - Likely a chapter in a book titled "Applications of Electroactive Polymers" published by Springer in 1993.
3. "Nickel metal hydride battery" - A webpage link to a specific product or information related to nickel metal hydride battery packs.
4. Tong B., Wang G., Zhang W., Wang C. "Node reclamation and replacement for long-lived sensor networks" - Appears to be a paper presented at the 6th Annual IEEE Communications Society Conference on Sensor, Mesh, and Ad Hoc Communications and Networks in 2009.
5. Kansal A., Hsu J., Zahedi S., Srivastava M. "Power management in energy harvesting sensor networks" - Published in ACM Transactions on Embedded Computing Systems in 2007.
6. Kansal A., Srivastava M. "An environmental energy harvesting framework for sensor networks" - Likely presented at the 2003 International Symposium on Low Power Electronics and Design.
7. Rahimi M., Shah H., Sukhatme G., Heideman J., Estrin D. "Studying the feasibility of energy harvesting in a mobile sensor network" - Appears to be a paper presented at the IEEE International Conference on Robotics and Automation in 2003.

АНТЕНА ДЛЯ ПОЛЬОВОГО РАДІОЗВ'ЯЗКУ

Федотов К.Ю., Сергієнко М.І., Кирпич М.С., Кононов А., Колошко І.В.

Радіотехнічний факультет КПІ ім. Ігоря Сікорського, Україна

Радіоклуб «Політехнік» КПІ ім. Ігоря Сікорського, Україна

E-mail: ux0un@ukr.net

ANTENNA FOR FIELD RADIO COMMUNICATION

The main task of this work is to increase the efficiency of radio communication in field conditions. After analyzing the task, it was decided to replace the standard antenna of the portable radio station with a remote antenna of higher efficiency. The starting point of the experiment was a half-wave dipole antenna.

Робота була виконана на замовлення сил оборони України. Оскільки на сьогоднішній день потреба в подібних пристроях дуже висока, будь-який різновид виробу може виявитися дуже корисним. Показано один із них, який було виконано на базі Радіоклубу КПІ.

Основне завдання даної роботи полягає в підвищенні ефективності радіозв'язку в польових умовах. Проаналізувавши поставлене завдання, було вирішено замінити штатну антену портативної радіостанції на виносну антену більшої ефективності. Відправною точкою експерименту стала напівхвильова дипольна антенна.

Опис експерименту. За основу нашої антени було взято конструкцію коаксіальної антени, яка описана в другому томі книги «Антени» К.Ротхаммель. Але в конструкцію були внесені деякі зміни:

1. Друге плече диполя ми виконали з оплетки того самого коаксіального кабеля на відміну від мідної трубки, що запропонована Ротхаммелем. Це технологічне рішення було втілене для забезпечення гнучкості конструкції та зручності транспортування;

2. До конструкції антени додали відсікаючий дросель, зроблений з кабелю шляхом його намотки на оправці діаметром 40 мм. Кількість витків – 4. Даний елемент дав змогу відсікти фідер від участі у випромінюванні. В результаті антенна стала більш захищеною від впливу радіозавад;

3. При виконанні вимірювань було визначено, що в такому варіанті антенна мала дуже вузьку смугу пропускання по $K_{CX}=3$. Для задоволення потреб зв'язку в польових умовах смуги пропускання по $K_{CX}=3$ 2 МГц виявилось замало. Тобто, виникла необхідність розширення смуги пропускання антени. Експериментальним шляхом було визначено, що при вкороченні нижнього елемента диполя у нас незначно змінилися показники активного та реактивного опорів, відповідно K_{CX} на резонансній частоті незначно збільшився від 1,1 до 1,25, але при цьому антенна стала надзвичайно широкопasmовою, що задовольнило вимоги технічного завдання.

Далі можна бачити змодельовану програмою MMANA GAL діаграму спрямованості запропонованої антени. Діаграма спрямованості є круговою, що дозволяє при розгортанні антени в умовах експлуатації не зважати на спрямування.

Також було побудовано графіки залежності K_{CX} від частоти, де визначено, що смуга пропускання антени по $K_{CX}=3$ сягає 20 МГц.

Виходячи з отриманих даних, було складено Порівняльну таблицю параметрів штатної та запропонованої антени. Отже, що ми бачимо:

- Коефіцієнт підсилення запропонованої антени більше, ніж у штатної;
- Смуга пропускання по КСХ=3 в два рази більше, ніж у штатної;
- Втрати у фідерній лінії запропонованої антени не перевищують 1,49 дБ, що під час експлуатації не є помітним;
- Діаграма спрямованості даної антени є круговою на відміну від штатної, котра залежить від положення відносно оператора.
- Відповідно до вище перелічених даних припускаємо, що дальність якісного зв'язку значно збільшиться у порівнянні зі штатною антеною.

Далі до вашої уваги представляю конструктивні матеріали даної антени.

Для виготовлення використано такі матеріали:

- Кабель RG-58 А/и «Одескабель»;
- Термозбіжна трубка;
- Кабельні пластмасові хомути;
- Кабельні обжимні роз'єми типу BNC.

Всі складові є доступними і економічно вигідними, що дозволяє виготовляти велику кількість виробів з мінімальними витратами на матеріали.

Наступним кроком представляю вам загальний вигляд готової антени. Як ми можемо бачити, що в згорнутому вигляді антена не займає багато місця та зручна в транспортуванні.

Пропоную вам переглянути відео практичного розміщення антени в умовах експлуатації (показ відео).

Після розгортання антени було проведено польові вимірювання її параметрів антенним аналізатором і виявилось, що ширина смуги пропускання по КСХ=3 є навіть більшою, ніж у розрахунку в MMANA GAL і сягає 37 МГц.

Надалі було порівняно рівні сигналу від джерела, розташованого на відстані 5 км, прийнятих на штатну та запропоновану антену. Вимірювання рівнів сигналу виконані за допомогою портативної радіостанції Motorola DP-4800. Спостерігаємо, що рівень сигналу із запропонованої антени становить -47 dBm, а зі штатної – 67 dBm.

Це підтверджує високу ефективність розробленої і виготовленої нами конструкції.

Виходячи з проведеної роботи, можна зробити **висновок**, що дані, отримані під час теоретичного моделювання, підтверджені на практиці. Виконано такі основні умови, як широкосмуговість та підвищення якості радіозв'язку.

Дана конструкція має **низку переваг**:

- Виготовлення цієї конструкції було значно спрощено та здешевлено порівняно з іншими наявними антенами для таких самих задач;
- Має значно меншу вагу, ніж інші антени, легка в розгортанні, зручна у використанні та транспортуванні.

Отже, дана антена має право на існування і може використовуватися для роботи в польових умовах. Ця конструкція особливо корисна, якщо є необхідність частого її розгортання і транспортування. На сьогоднішній день дана антена вже протестована замовниками і має гарні відгуки.

Література

1. Антенни. Карл Ротхаммель., Том 2 . 2005. – 416 с.

РОЗВИТОК МЕТОДІВ СИНХРОНІЗАЦІЇ ДЛЯ МОБІЛЬНИХ СЕНСОРНИХ МЕРЕЖ

¹Кожухар І.В., ¹Лисенко О.І., ¹Гетьман О.В., ¹Новіков В.І., ²Фуртат О.В.

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

²Таврійський національний університет імені В. І. Вернадського, Україна

E-mail: novikov1967@ukr.net

DEVELOPMENT OF SYNCHRONIZATION METHODS FOR MOBILE SENSOR NETWORKS

A new synchronization method is proposed for mobile sensor networks that combines internal and external synchronization to achieve improved results in synchronization accuracy and efficiency.

Мобільні сенсорні мережі (МСМ) стають все більш популярними у різних галузях застосування [1-3]. МСМ можуть використовуватись у різних галузях, особливо там, де існує складність або недоцільність використання традиційних мереж. Широкий вибір доступних датчиків та механізмів, легкість у встановленні та експлуатації, компактність та відносно низька вартість допомагають у поширенні та розвитку МСМ.

МСМ є розподіленими системами, в яких у кожного сенсорного вузла є свій власний годинник і власне уявлення про час. Тим не менш, загальна шкала часу серед сенсорних вузлів важлива для визначення причинного зв'язку між подіями у фізичному середовищі, щоб підтримати усунення надлишкових сенсорних даних і в цілому, полегшити функціонування МСМ. Оскільки кожен вузол в сенсорній мережі функціонує самостійно і покладається на свій власний годинник, показання годинників різних сенсорних вузлів будуть відрізнятися. Таким чином, потрібна синхронізація часу (або годинника) для забезпечення того, щоб час зчитування, значною мірою, можна було порівняти [4].

У той час, як методи синхронізації часу для проводових мереж отримали значну кількість уваги, ці методи не застосовні для МСМ через унікальні проблеми, пов'язані з оточенням (конфігурацією, умовами експлуатації) сенсорів МСМ. Ці проблеми включають потенційно більший масштаб МСМ, необхідність в автоматичній конфігурації та надійності, а також потреба збереження енергії. Також більшість методів, які вже запропоновані на сьогоднішній день для синхронізації часу в стаціонарних безпроводових сенсорних мережах (БСМ) не враховують мобільність сенсорних вузлів [4].

У доповіді пропонується комбінований метод внутрішньо-зовнішньої синхронізації, що дозволяє підвищити точність синхронізації часу для МСМ.

Основна ідея запропонованого методу полягає в реалізації синхронізації мобільного сенсорного вузла зі стаціонарним сенсорним вузлом в наступних умовах. Сенсори в мережі будуть синхронізуватися між собою за допомогою методу внутрішньої синхронізації, а мобільний приймач вже буде синхронізуватися з головними вузлами кластерів МСМ за допомогою методу зовнішньої синхронізації (рис. 1).

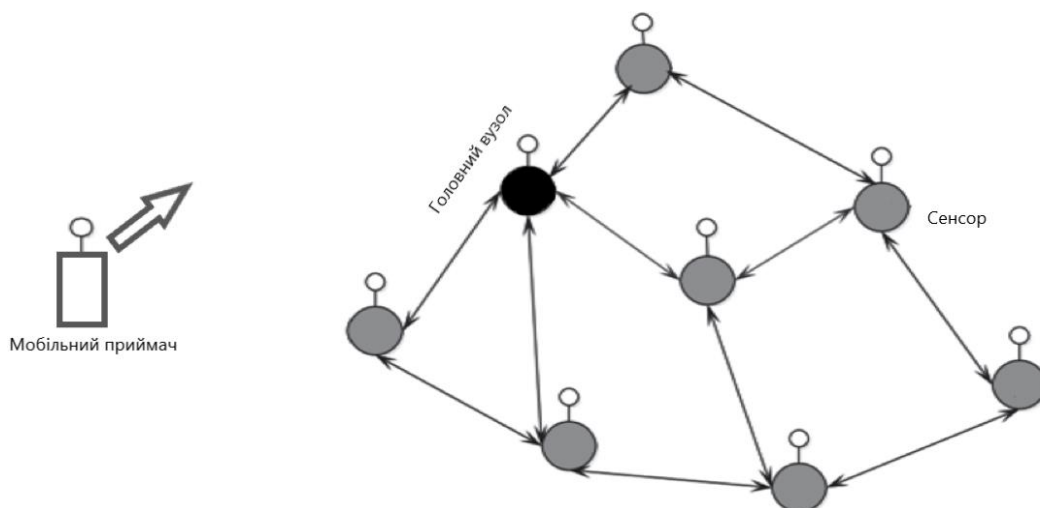


Рис.1. Топологія МСМ, для якій пропонується метод внутрішньо-зовнішньої синхронізації.

Внутрішня синхронізація в МСМ відноситься до процесу, коли годинники всіх вузлів у мережі налаштовуються так, щоб вони були у взаємній узгодженості, незалежно від будь-яких зовнішніх системних годинників. Це означає, що всі вузли в мережі мають спільне розуміння часу, навіть якщо цей час може відрізнятися від зовнішніх опорних точок відліку часу. З іншого боку, зовнішня синхронізація включає налаштування годинників всіх вузлів у відповідності з зовнішнім джерелом часу або системним годинником.

Внутрішня синхронізація зазвичай використовується для забезпечення правильної роботи системи, тоді як зовнішня синхронізація в основному використовується для надання користувачам зручної інформації про контроль часу. Важливо відзначити, що внутрішня синхронізація може виконуватися в "рівноправному" режимі або в режимі "ведучий-ведений". Зовнішня синхронізація не може виконуватися одноранговим способом; для неї потрібен майстер-вузол, який зв'язується зі службою часу, наприклад GPS, для синхронізації ведених пристроїв і самого себе з контрольним часом.

Внутрішня синхронізація

Локальне керування часом: Сенсорні пристрої можуть мати свої внутрішні генератори часу або годинники для виконання операцій відповідно до власних графіків.

Самостійне управління подіями: Вони можуть реагувати на власні події (наприклад, зчитування даних з сенсорів, внутрішні операції тощо) без залучення зовнішніх джерел.

Зовнішня синхронізація

Синхронізація здійснюється через базові станції мобільного зв'язку: Вони можуть використовувати сигнали від мережі мобільного зв'язку для синхронізації часу або отримання інформації про таймінг.

Використання точок доступу Wi-Fi: Wi-Fi точки доступу також можуть надавати можливості синхронізації для сенсорних пристроїв.

Глобальні часові служби, такі як GPS: Вони можуть використовувати сигнали від систем позиціонування (наприклад, GPS) для синхронізації часу та отримання глобальної інформації про місцезнаходження.

Комбінування цих методів синхронізації дозволяє досягти більшої точності та ефективності синхронізації в мобільних сенсорних мережах. Наприклад, внутрішня синхронізація може бути корисною для швидкого реагування на події, які відбуваються на пристрої, тоді як зовнішня синхронізація забезпечує глобальну узгодженість часу та дій між різними пристроями в мережі.

Таким чином, у доповіді запропоновано новий метод синхронізації для МСМ, який поєднує внутрішню і зовнішню синхронізацію для досягнення покращення результатів у точності та ефективності синхронізації. Напрямом подальших досліджень є оцінка ефективності запропонованого методу за різних параметрів та умов функціонування МСМ.

Література

1. Ільченко М.Ю., Кравчук С.О. Телекомунікаційні системи. – Київ: Наукова думка, 2017. – 730 с. Досягнення в телекомунікаціях 2019 / за наук. ред. М.Ю.Ільченка, С.О.Кравчука: монографія. - Київ: Інститут обдарованої дитини НАПН України, 2019.- 336 с.
2. Міночкін А.І., Романюк В.А., Жук О.В. Перспективи розвитку тактичних сенсорних мереж// Збірник наукових праць №4. – К.: ВІТІ НТУУ “КПІ”. – 2007. – С. 112 – 119.
3. Лисенко О.І., Романченко І.С., Чумаченко С.М., Данилюк С.Л., Новіков В.І., Тачиніна О.М., Кірчу П.І., Валуйський С.В. Моделі застосування інформаційно-телекомунікаційних технологій на основі безпілотних авіаційних комплексів у надзвичайних ситуаціях. – К.: НАУ, 2016. – 332 с.
4. Sundararaman, B., Buy, U., and Kshemkalyani, A.D. (2005) Clock synchronization for wireless sensor networks: A survey. *Ad Hoc Networks* 3 (3), 281–323.

АВТОМАТИЗАЦІЯ РОБОТИ ДАТАЦЕНТРУ З ВИКОРИСТАННЯМ МАШИННОГО НАВЧАННЯ

Кравченко І.М., Міночкін Д.А.

*Навчально-науковий інститут телекомунікаційних
систем, КПІ ім. Ігоря Сікорського, Україна
E-mail: il.kravchenko115@gmail.com*

AUTOMATION OF DATA CENTRE OPERATIONS USING MACHINE LEARNING

The main trends in the application of process automation using machine learning for data centers are summarised. The results of a neural network for determining fire hazards in data centres are presented.

Використання розвиваючого штучного інтелекту в датацентрах для автоматизації роботи відкриває безліч можливостей і обіцянок щодо значного прориву в інфраструктурі цих об'єктів. Ось деякі з переваг, які може принести впровадження розвиваючого штучного інтелекту в датацентри:

Покращена ефективність роботи. Штучний інтелект здатен аналізувати великі обсяги даних швидше і ефективніше, ніж людський персонал. Це дозволяє автоматизувати багато процесів у датацентрі, зменшуючи час і зусилля, потрібні для управління та моніторингу.

Прогнозування та попередження відмов. Завдяки аналізу даних і використанню алгоритмів машинного навчання, розвиваючий штучний інтелект може прогнозувати можливі відмови обладнання та попереджати їх, дозволяючи здійснювати ремонти або заміни до виникнення серйозних проблем.

Оптимізація ресурсів. Інтелектуальні алгоритми можуть допомагати оптимізувати використання ресурсів у датацентрі, зокрема енергії, обчислювальних можливостей і мережевої пропускної здатності. Це допомагає зменшити витрати та підвищити продуктивність.

Виявлення аномалій і кібербезпека. Штучний інтелект може виявляти незвичайні патерни або аномальну поведінку в мережах датацентрів, що

допомагає вчасно реагувати на потенційні загрози кібербезпеки та уникати серйозних проблем.

Зниження ризику людських помилок. Автоматизація за допомогою штучного інтелекту дозволяє уникнути багатьох помилок, які можуть виникнути через людський фактор, що забезпечує більшу надійність і стабільність роботи датацентра.

Швидкість реакції та скорочення часу вирішення проблем. Завдяки аналізу в реальному часі і автоматичному управлінню, розвиваючий штучний інтелект дозволяє операторам датацентру швидко реагувати на проблеми і вирішувати їх ефективно.

Загалом, використання розвиваючого штучного інтелекту в датацентрах для автоматизації роботи має потенціал стати вагомим проривом в інфраструктурі, що дозволить покращити продуктивність, забезпечити безпеку і ефективність роботи цих важливих технологічних об'єктів. В серії робіт [3][4], досліджується можливість автоматизувати і побудувати новітні дата центри за допомогою штучного інтелекту і машинного навчання.

В даній доповіді, використано класифікаційні моделі для побудови нейронної мережі для забезпечення пожежної безпеки. Дана модель навчена за допомогою реального набору даних[2] з сенсорів які на вході отримують інформацію про вміст частинок в диму. І на основі цих даних буде натреновано нейронну мережу для розпізнавання в цих даних пожежну безпеку.

В цій частині доповіді буде показано як провести аналіз вхідних даних для виявлення взаємозв'язків, патернів, аномалій та загального розуміння структури даних. Найбільша увага буде приділена обробці даних для подальшого використанню в навчанні мережі, для визначення та обробки відсутніх значень у даних для забезпечення якості та достовірності аналізу та показати залежності між змінними – яка змінна впливає на результат того чи буде пожежна безпека чи ні.

І на основі попередніх даних була побудована нейронна мережа з

використанням різних алгоритмів класифікації. І на виході ми отримали навчену мережу яка зможе сама розпізнавати чи є у нас пожежна небезпека в датацентрі.

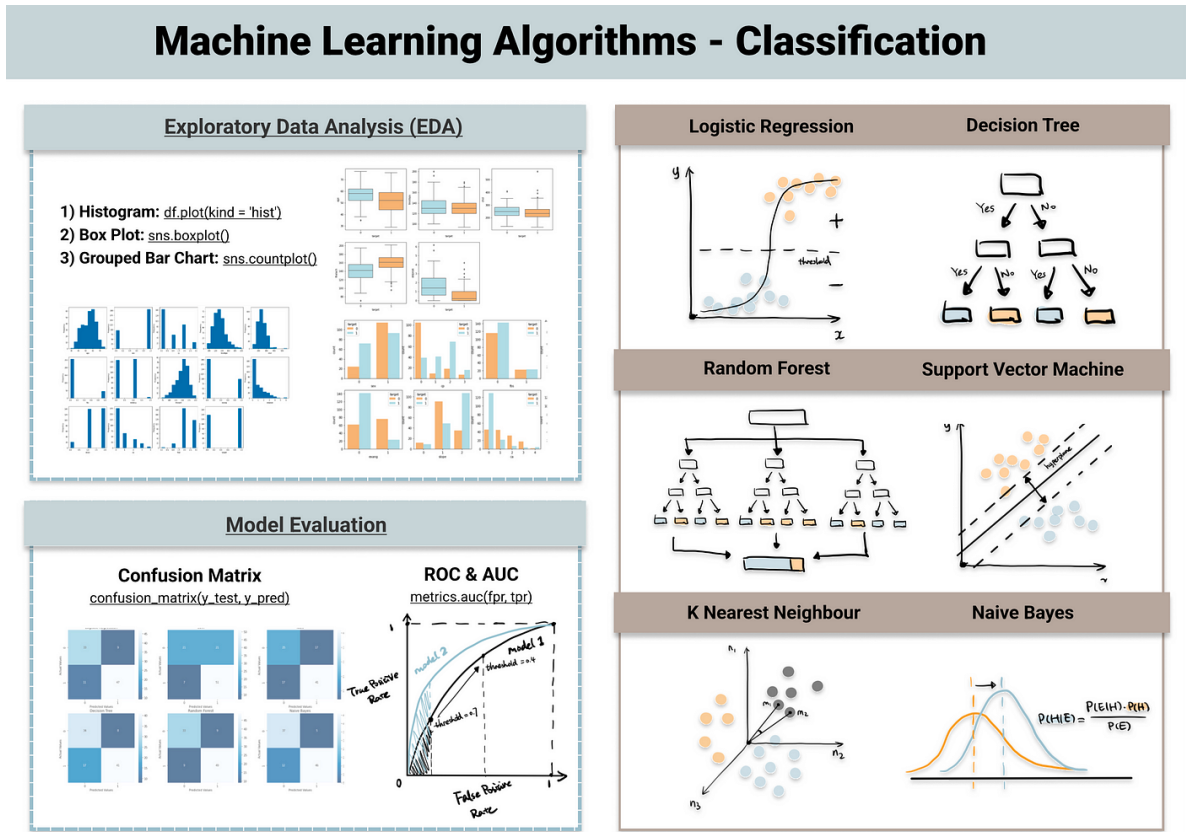


Рис.1. Алгоритми Машинного навчання – Класифікаційні [1].

Література

1. Gong D. Top 6 Machine Learning Algorithms for Classification. *Medium*. URL: <https://towardsdatascience.com/top-machine-learning-algorithms-for-classification-2197870ff501> (date of access: 23.03.2024).
2. Smoke Detection Dataset. *Kaggle: Your Machine Learning and Data Science Community*. URL: https://www.kaggle.com/datasets/deepcontractor/smoke-detection-dataset?select=smoke_detection_iot.csv (date of access: 23.03.2024).
3. Chang S. S., Chen O. W., Varshney S. Autonomous Datacenter: Datacenter That Runs Itself and Heals Itself. De Gruyter, Inc., 2020. 300 p.
4. Machine Learning Empowered Intelligent Data Center Networking / T. Wang et al. Singapore : Springer Nature Singapore, 2023. URL: <https://doi.org/10.1007/978-981-19-7395-6> (date of access: 23.03.2024).

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ СТИСКУ ДАНИХ В БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ

Третяк А.В., Лисенко О.І.

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна
E-mail: petbka.tasher@gmail.com*

COMPARATIVE ANALYSIS OF DATA COMPRESSION METHODS IN WIRELESS SENSOR NETWORKS

The article analyzes various methods of data compression used in wireless sensor networks. Four main categories are considered: string-based compression, image-based compression, distributed source coding, and compressed sensing. Comparison of these methods for data recovery, lossless or lossy. Algorithms in each category are given, and their principle of action is explained.

Бездротова сенсорна мережа (WSN) складається з одного або декількох віддалених приймачів і великої кількості сенсорних вузлів. Кожен сенсорний вузол є компактним бездротовим пристроєм, який безперервно збирає навколишню інформацію та передає дані датчиків приймачам за допомогою схеми множинної маршрутизації з кількома переходами [1]. WSN відкривають нові можливості для повноцінного обчислення та контекстуального моніторингу фізичного середовища. Зазвичай їх використовують для спостереження за конкретними явищами або відстеження об'єктів. Практичні застосування WSN включають, наприклад, моніторинг тварин, трансформацію сільського господарства, охорону здоров'я, спостереження всередині приміщень та розумні будівлі.

Для зменшення обсягу даних від датчиків необхідно їх стиснути у мережі. В залежності від можливості відновлення даних, можна виділити стиснення: без втрат, із втратою. Стиснення без втрат позначає, що після проведення операції декомпресії ми отримуємо точно такі ж дані, як і до стиснення. Один із стандартних прикладів - це кодування Хаффмана [2]. Стиснення з втратою означає втрату деяких деталей даних через операцію стиснення. До цієї категорії відноситься більшість схем стиснення зображень і відео, таких як JPEG2000 [3].

Методи стиснення даних у WSN, можна класифікувати на категорії: стиснення на основі рядків, стиснення на основі зображень, стиснення за кодуванням розподіленого джерела, стиснутого зондування.

1) Методи стиснення на основі рядків розглядають дані датчиків як послідовність символів, а потім застосовують схеми стиснення даних, які

використовуються для обробки текстових даних, щоб стиснути ці дані датчиків. Успадковані від цих схем стиснення текстових даних методи стиснення на основі рядків також можуть забезпечити стиснення без втрат.

Прикладом може бути алгоритм Lempel-Ziv-Welch (LZW) [4] який динамічно створює словник для кодування нових рядків на основі рядків, які зустрічалися раніше. Відправник, і одержувач мають однакові початкові словникові статті, а всі нові словникові статті можуть бути отримані з існуючих словникових статей і потоку вхідних даних. Спочатку він сканує вхідний потік символів, доки не знайде підрядок, відсутній у словнику. Кодує найдовшу знайдену підрядку індексом відповідності у словнику. Додає цю нову підрядок до словника з черговим доступним кодом. Процес повторюється під час сканування наступних символів вхідного потоку

2) Методи стиснення на основі зображень організовують WSN в ієрархічну архітектуру, а потім застосовують деякі схеми стиснення зображень, такі як вейвлет-перетворення, щоб забезпечити багаторазову роздільну здатність даних зондування всередині мережі. Деякі другорядні функції даних зондування можуть бути втрачені через операції стиснення, тому метод стиснення на основі зображення підтримує стиснення з втратою.

Зображення зазвичай складається з багатьох малих пікселів, і його можна представити у вигляді матриці, де кожен елемент відображає значення одного пікселя. Застосовуючи вейвлет-перетворення до цієї матриці, можна виділити ключові характеристики зображення в частотному діапазоні. В результаті розмір зображення може бути значно зменшений, зберігаючи лише важливі характеристики. Підходи до стиснення даних на основі зображень використовують подібний підхід. Вони організовують бездротову сенсорну мережу в ієрархічну структуру і розглядають дані зондування, надіслані всіма вузлами датчиків, як зображення з кількома пікселями. Після цього застосовується вейвлет-перетворення для отримання просторового та часового узагальнення цих даних зондування. У випадку, коли дані зондування мають високу просторову або часову кореляцію, методи стиснення на основі зображень можуть додатково зменшити обсяг передаваних даних. Нижче описані методи стиснення на основі зображень: структура DIMENSIONS [5] і структура стиснення та запитів із різною роздільною здатністю MRCQ [6].

Метод стиснення даних DIMENSIONS:

1. Використовує ієрархічну архітектуру бездротової сенсорної мережі.
2. Розбиває мережу на кластери, у кожному вибирається головний вузол.
3. Головні вузли збирають дані з датчиків та виконують стиск.
4. Застосовується 3D дискретне вейвлет-перетворення для просторово-

часового підсумовування даних.

5. Дані на нижніх рівнях ієрархії мають кращу роздільну здатність.

6. Дані на верхніх рівнях - грубішу роздільну здатність, але менший обсяг.

7. Дозволяє запитувати дані з потрібним дозволом у різних головних вузлів.

Основна перевага полягає в ефективному стисненні великих обсягів корельованих даних датчиків, тому DIMENSIONS добре підходить для стиснення просторово-часових даних датчиків у великих сенсорних мережах. Недолік порівняно з MRCQ - висока обчислювальна складність.

Метод стиснення даних MRCQ (multi-resolution compression and query):

1. Використовує ієрархічну архітектуру бездротової сенсорної мережі.

2. Розбиває мережу на кластери та рівні, у кожному кластері вибирається вузол обробки даних.

3. Вузли нижнього рівня застосовують 2D дискретне косинусне перетворення.

4. Вузли верхніх рівнів передають лише частину найбільш значимих перетворених даних.

5. Дозволяє отримувати дані з різною роздільною здатністю на різних ієрархічних рівнях.

3) Методи кодування розподіленого джерела стискають дані зондування всередині мережі згідно з теоремою Слепяна-Вольфа, яка доводить, що два або більше корельованих потоків даних можуть бути закодовані незалежно, а потім спільно декодовані в приймачі зі швидкістю, що дорівнює їхній спільній ентропії. Таким чином, розподілені методи кодування джерела можуть підтримувати стиснення без втрат [7].

Метод розподіленого вихідного кодування - базується на теоремі Слепяна-Вольфа, яка показує, що при кодуванні двох чи більше корельованих джерел даних, кожне з яких кодується незалежно, а потім спільно декодується, можливо досягти стиснення даних без втрат зі швидкістю бітів, що дорівнює їх спільній ентропії. Він дозволяє сенсорним вузлам стискати дані зондування без кооперації та узгодження між собою, але вимагає попереднього знання кореляції в даних. Застосовується для стиснення даних зондування в бездротових сенсорних мережах у випадках, коли є корельовані потоки даних від різних сенсорних вузлів.

4) Методи стиснутого зондування вказують на те, що будь-які досить стислі дані можна точно відновити з невеликої кількості неадаптивних рандомізованих вибірок лінійної проекції. Таким чином, вони можуть використовувати стиснення, не покладаючись на будь-які попередні знання

або припущення щодо даних зондування. З огляду на наведене вище спостереження, методи стиснення можуть забезпечити стиснення без втрат [8].

Метод стиснутого зондування - використовує стисливість даних без покладання на конкретні припущення щодо даних чи їх кореляцій. Базується на теорії стисненого сприйняття, згідно з якою будь-які достатньо стислі дані можна точно відновити з невеликої кількості випадкових лінійних проєкцій цих даних. Для розріджених даних з невеликою кількістю ненульових елементів цей метод дозволяє отримати їх стиснений набір зі значно меншою розмірністю. Даний метод дозволяє здійснити стиснення даних без втрат без попередньої обробки та координації між сенсорними вузлами.

Коротка порівняльна характеристика цих методів наведена в таблиці 1

Таблиця 1. Коротка порівняльна характеристика методів.

<i>Метод</i>	<i>Категорія стиснення</i>	<i>Відновлення даних</i>	<i>Теорія стиснення</i>
LZW	На основі рядків	Без втрат	-
DIMENSIONS	На основі зображення	З втратами	Вейвлет-перетворення
MRCQ	На основі зображення	З втратами	Вейвлет-перетворення
Розподілене кодування	Розподілене вихідне кодування	Без втрат	Теорема Слепяна-Вольфа
Зондування	Зондування	Без втрат	Зондування

Література

1. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Comm. Magazine, vol. 40, no. 8, pp. 102–114, 2002.
2. M. Nelson and J. L. Gailly, The data compression book.
3. D.S. Taubman and M.W. Marcellin, JPEG2000: Standard for Interactive Imaging.
4. T.A. Welch, "A technique for high-performance data compression," Computer, vol. 17, no. 6, pp. 8–19, 1984.
5. D. Ganesan, B. Greenstein, D. Estrin, J. Heidemann, and R. Govindan, "Multiresolution storage and search in sensor networks," ACM Trans. Storage, vol. 1, no. 3, pp. 277–315, 2005.
6. Y.C. Wang, Y.Y. Hsieh, and Y.C. Tseng, "Multiresolution spatial and temporal coding in a wireless sensor network for long-term monitoring applications," IEEE Trans. Computers, vol. 58, no. 6, pp. 827–838, 2009.
7. Z. Xiong, A.D. Liveris, and S. Cheng, "Distributed source coding for sensor networks," IEEE Signal Processing Magazine, vol. 21, no. 5, pp. 80–94, 2004.
8. J. Haupt, W.U. Bajwa, M. Rabbat, and R. Nowak, "Compressed sensing for networked data," IEEE Signal Processing Magazine, vol. 25, no. 2, pp. 92–101, 2008.

ВИЯВЛЕННЯ СИГНАЛУ РУХОМОЇ ЦІЛІ FMCW РАДАРМ ПРИ ВІДОМІЙ ПОТУЖНОСТІ ЗАВАДИ

Маленчик Т.В., Жук С.Я.
Радіотехнічний факультет
КПІ ім. Ігоря Сікорського, Україна
E-mail: sparrow@.ex.ua.

SIGNAL DETECTION OF MOVABLE TARGET BY FMCW RADAR WITH KNOWN INTERFERENCE POWER

An algorithm for detecting a moving target signal by FMCW radar with known power interference was obtained and its efficiency was analyzed.

Одним з перспективних засобів виявлення рухомих цілей в тому числі і малорозмірних БПЛА є FMCW (Frequency modulated continuous wave) радар [1]. Він забезпечує: високоточне вимірювати дальності, а також радіальної швидкості, кращу безпеку через відсутність імпульсного випромінювання з великою потужністю; низьке енергоспоживання [2].

Для виявлення сигналу цілі на далекомірно-доплерівському портреті за даними FMCW радару широко використовуються алгоритми сімейства CFAR (Constant False Alarm Rate) [3]. При цьому потужність завади вважається невідомою і постійно оцінюється, шляхом аналізу відліків в межах прямокутної ковзної області. Оцінка ефективності таких алгоритмів проводиться шляхом статистичного моделювання. Представляє інтерес розробка алгоритму виявлення сигналу цілі при відомій потужності завади. Такий алгоритм забезпечує потенційні характеристики виявлення цілі.

Обробка сигналу FMCW радару включає прийом відбитого від цілі сигналу, його перемноження з опорним сигналом в змішувачі, низькочастотну фільтрацію результату перемноження з подальшим перетворенням в цифрову форму. В процесі виявлення цілі на інтервалі когерентного накопичення розглядаються дві гіпотези:

$$\begin{aligned} H_1: x(n\Delta t, mT) &= A \cos(2\pi f n + 2\pi F m + \phi) + w(n\Delta t, mT), \\ H_0: x(n\Delta t, mT) &= w(n\Delta t, mT), \quad n = \overline{0, N-1}, m = \overline{0, M-1}, \end{aligned} \quad (1)$$

де A - амплітуда; ϕ - початкова фаза; f , F - різницева частота зондуючого і отриманого сигналів та доплерівський зсув частоти цілі

$$f = \frac{2\rho R}{c}, \quad F = \frac{2f_c \nu n}{c};$$

ρ - швидкість зміни частоти ЛЧМ-сигналу; R - дальність до цілі; f_c - носійна частота; ν - радіальна швидкість цілі; c - швидкість світла; Δt - крок дискретизації демодульованого сигналу; T - період модуляції ЛЧМ-сигналу; $w(n\Delta t, mT)$ - дискретний білий гаусівський шум з відомою дисперсією σ^2 .

Амплітуда A , частоти f, F та початкова фаза ϕ є невідомими. Будемо вважати, що на інтервалі когерентного накопичення ціль знаходиться в межах одного елемента розрізнення за дальністю і радіальною швидкістю. В цьому випадку частоти f, F на інтервалі спостереження не змінюються.

В якості критерію оптимальності використовується критерій Неймана-Пірсона, який при заданій ймовірності хибної тривоги α забезпечує максимальну ймовірність правильного виявлення D . Розглянута задача відноситься до класу задач виявлення з параметричної апріорною невизначеністю. Застосуємо для її вирішення адаптивний підхід з використанням методу максимальної правдоподібності [3]. В даному підході при відомому вимірюванні $x(n, m), n = \overline{0, N-1}, m = \overline{0, M-1}$ за критерієм максимальної правдоподібності визначаються оцінки невідомих параметрів., які в подальшому використовуються при визначенні функції правдоподібності гіпотези H_1 при вирішенні задачі виявлення. Можна показати, що вирішальне правило виявлення має вигляд:

$$\Gamma(\hat{f}_k, \hat{F}_l) \underset{\hat{H}_0}{\overset{\hat{H}_1}{\geq}} \gamma \quad (2)$$

де $\Gamma(f_k, F_l), k = \overline{0, N-1}, l = \overline{0, M-1}$ – періодограма, що розраховується шляхом двомірного дискретного перетворення Фур'є від сигналу $x(n\Delta t, mT)$

$$\Gamma(f_k, F_l) = \frac{1}{NM} \left| \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} x(n\Delta t, mT) \exp(-i2\pi(f_k n\Delta t + F_l mT)) \right|^2,$$

\hat{f}_k, \hat{F}_l - значення частот f_k, F_l , при яких періодограма $\Gamma(f_k, F_l)$ приймає максимальне значення.

Ймовірність хибної тривоги розраховується за формулою:

$$\alpha = P\{\Gamma(f, F) > \gamma | H_0\} = P_{\chi^2_2} \left(\frac{2\gamma}{\sigma^2} \right) = \int_{2\gamma/\sigma^2}^{\infty} \frac{1}{2} e^{-x/2} dx = \int_{\gamma/\sigma^2}^{\infty} \frac{1}{2} e^{-z} dz = e^{-\gamma/\sigma^2}, \quad (3)$$

$p_{\chi^2_2}(\cdot)$ - центральний розподіл хі-квадрат з двома ступенями свободи.

Тоді оптимальне значення порогу визначається за формулою:

$$\gamma = \sigma^2 \ln \left(\frac{1}{\alpha} \right). \quad (4)$$

Знайдемо ймовірність правильного виявлення D :

$$D = P\{\Gamma(f, F) \geq \gamma | H_1\} = P_{\chi^2_2(\lambda)} \left(\frac{2\gamma}{\sigma^2} \right) = Q_M \left(\sqrt{\frac{NMA^2}{2\sigma^2}}; \sqrt{\frac{2\gamma}{\sigma^2}} \right), \quad (5)$$

де $p_{\chi_2^2}(\circ)$ - нецентральний розподіл хі-квадрат з двома ступенями свободи; $Q_M(\circ)$ – функція Маркума.

Залежності ймовірності правильного виявлення цілі D від ВСШ (відношення сигнал шум) h^2 при $\alpha=10^{-3}$, розраховані за формулою (5) зображені на рис.1 суцільними лініями. При цьому ВСШ розраховується за формулою

$$h^2 = 10 \log\left(\frac{NMA^2}{2\sigma^2}\right).$$

Також на рис.1 штриховими лініями наведені аналогічні залежності, отримані шляхом статистичного моделювання, які співпадають з теоретичними розрахунками.

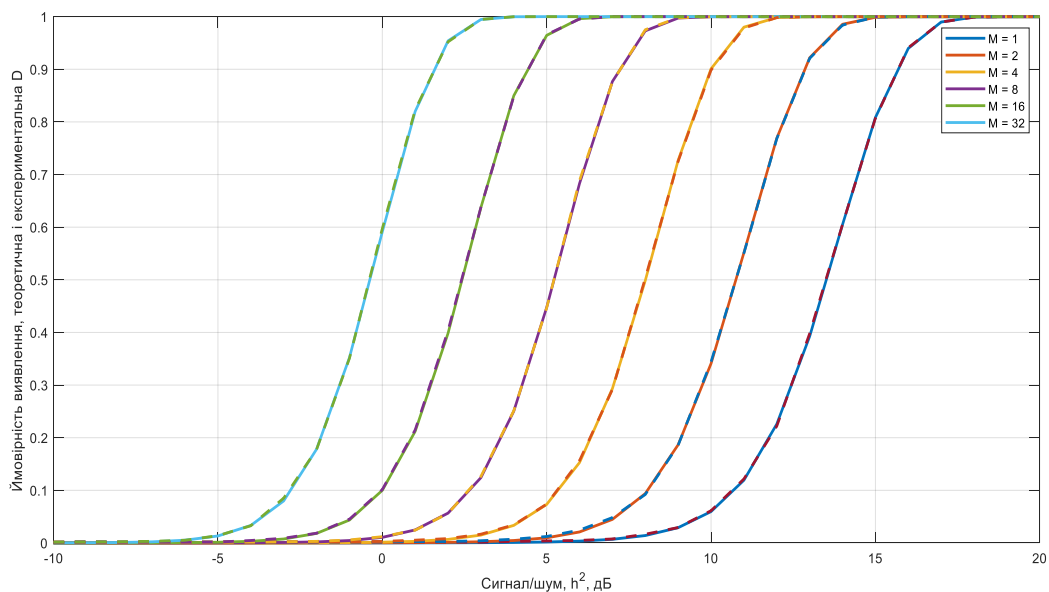


Рис. 1.- Залежності ймовірності правильного виявлення цілі D від ВСШ h^2 .

При збільшенні періодів зондування в два рази, необхідне для досягнення тієї ж ймовірності D ВСШ h^2 зменшується на 3 дБ, що відповідає закономірності когерентного накопичення сигналів. Отримані характеристики можуть виступати в якості нижньої границі ймовірності D алгоритмів виявлення сімейства CFAR.

Література

1. Jin, Y., Kim, B., Kim, S., & Lee, J. (2018). Design and Implementation of FMCW Surveillance Radar Based on Dual Chirps. *Elektronika Ir Elektrotechnika*, 24(6), 60-66. <https://doi.org/10.5755/j01.eie.24.6.22292>
2. Mohinder Jankiraman, *FMCW Radar Design*, Artech, 2018.
3. Richards, Mark A. 2022. *Fundamentals of Radar Signal Processing*. 3rd ed.

ПРОГРАМНО-АПАРАТНИЙ КОМПЛЕКС АДАПТИВНОГО МОНІТОРИНГУ ОБМЕЖЕНОЇ ЕКОСИСТЕМИ

Сукало М.Л., Чумаченко С.М.

Національний університет харчових технологій, Київ, Україна

E-mail: biginhunter@gmail.com

PROGRAMMABLE HARDWARE COMPLEX FOR ADAPTIVE MONITORING OF RESTRICTED ECOSYSTEM

In the course of the research, a new software and hardware complex was proposed, developed and modeled, which is intended for monitoring restricted ecosystems in areas of anthropogenic pollution.

У сучасних умовах, коли Україна стикається з рядом складних викликів в галузі екології та безпеки, стає дедалі більш актуальною проблема розробки комплексних методів моніторингу обмежених екосистем (ОЕС). Наряду із загальними умовами спостереження ці методи повинні адаптуватися до специфіки об'єктів, що потребують моніторингу, таких як території, які постраждали від стихійного лиха, бойових дій, об'єкти критичної інфраструктури (ОКІ) та потенційно небезпечні об'єкти (ПНО). Дослідження можливостей створення мультисенсорної системи веде до розробки прототипу готового рішення, призначеного для забезпечення високого рівня безпеки та запобігання виникненню надзвичайних ситуацій в місцях, де існує потенційна загроза для здоров'я та життя людей. Такими зонами є території ведення бойових дій, ПНО, ОКІ. Серед ПНО можна виділити території біля атомних станцій таких як Чорнобильська АЕС, Запорізька АЕС та інші промислові об'єкти що попали в зону бойових дій.

На сьогодні існує ряд рішень, спрямованих на екологічний моніторинг та передбачення стихійних небезпек. Проте відсутнє універсальне рішення, спрямоване на проведення адаптивного моніторингу ОЕС біля ПНО та ОКІ і прилеглих територіях. Невиявлені вчасно місця техногенного забруднення можуть призвести до поширення небезпечних речовин на прилеглі території. Використання сучасних приладів та механізмів може вирішити проблему моніторингу екологічного стану в Україні та вчасного виявлення проблемних зон.

Ринок спеціалізованих моніторингових систем розвивається, і наразі обмежена кількість компаній пропонує готові до впровадження технології. Однією з таких відомих компаній є Benish GPS, яка є міжнародним постачальником GPS-рішень для різних типів користувачів. Компанія використовує методологію створення систем, яка включає об'єднання датчиків та передачу інформації з них через спеціально розроблений додаток для відслідковування різних процесів. Ідея таких апаратно-програмних рішень наближена до теми дослідження, але, на жаль, компанія не має

універсального механізму, що міг би адаптуватись для критичного моніторингу ОЕС об'єкту спостереження.

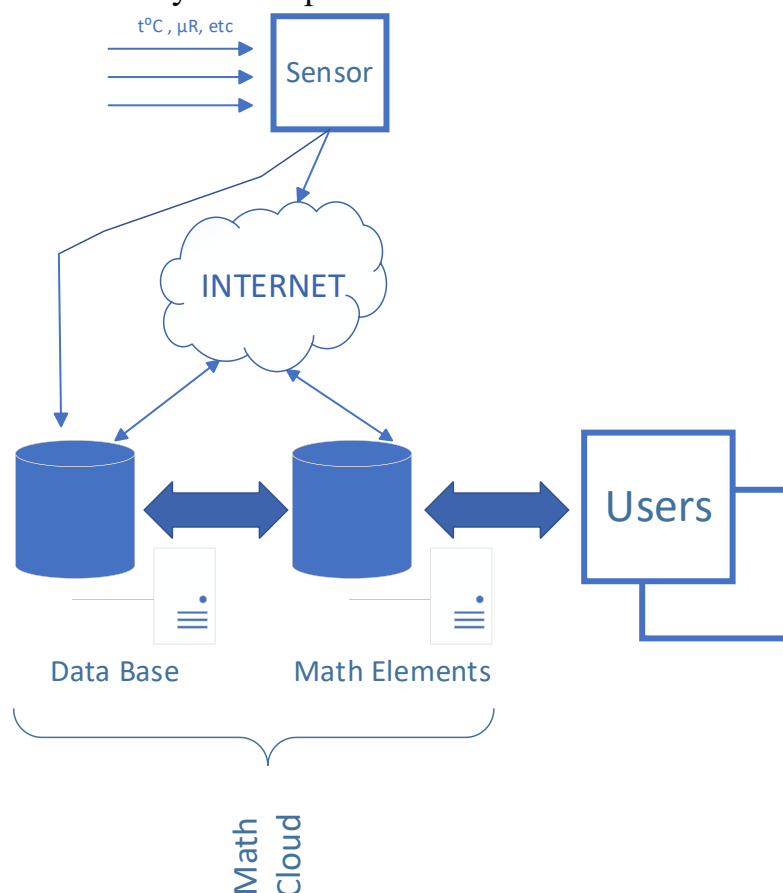


Рис. 1. Структурна схема розподілу функцій системи моніторингу ОЕС.

Склавши всі блоки модельованого апаратно-програмного комплексу, отримуємо готове до впровадження рішення, яке складається з трьох ключових компонентів: модуля збору та передачі даних, модуля трансферу даних з локального середовища до мережі Інтернет, а також веб-орієнтованої системи моніторингу для збереження та відображення даних.

Отримання очікуваного результату досліджень здійснюється через збір актуальної інформації про зовнішнє середовище програмованим мікроконтролером "MCU", який може бути розташований як на людині так і на різних мобільних механізованих платформах.

Важливим є те, що "MCU" не залежить безпосередньо від характеристик носія, тому може використовуватися будь-яка форма слідування програмованим маршрутом

Очікуваний ефект від впровадження мультисенсорної системи полягає в ранньому виявленні факторів надзвичайних ситуацій, прогнозуванні та прийнятті рішень щодо ліквідації виниклої небезпеки, а також невідкладному залученні до реагування відповідних підрозділів ДСНС України та інших державних структур. Простий механізм реалізації системи забезпечить подальшу масштабованість та можливість швидкої заміни ключових елементів.

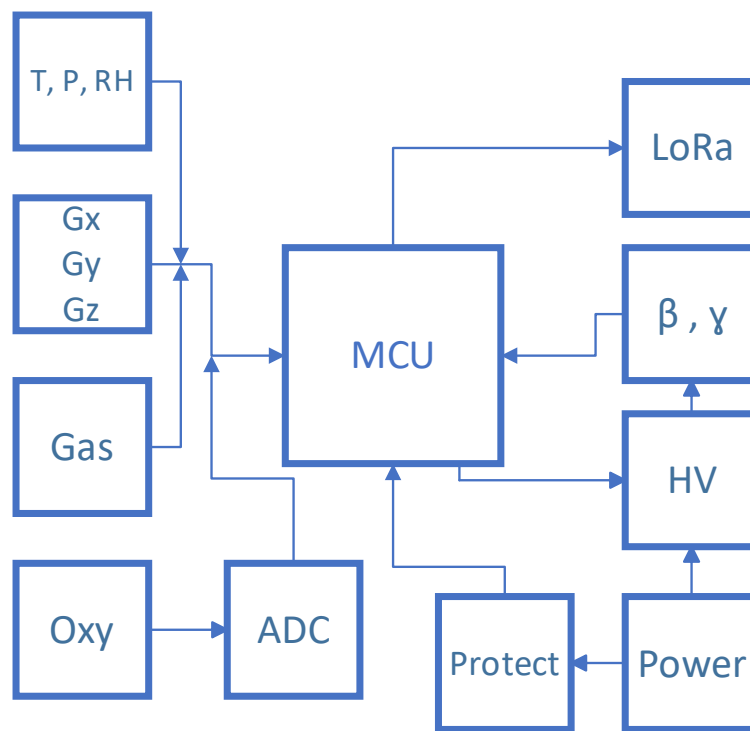


Рис 2 Підключення периферійних пристроїв до МК

Під час розгляду проблеми було встановлено, що методи дослідження адаптивного моніторингу ОЕС на ПНО та ОКІ, що використовуються спеціальними службами, не є достатньо ефективними. Замість цього був запропонований та змодельований апаратно-програмний комплекс, який дозволяє реалізувати набір інструментів, спеціально пристосованих для моніторингу ОЕС в зонах техногенного забруднення.

Література

1. Ran Liuab, Chau Yuenb, Tri-Nhut Doc, Meng Zhangd, Yong Liang, GuaneU-XuanTanb. Cooperative positioning for emergency responders using self IMU and peer-to-peer radios measurements. *Information Fusion*. April 2020. Volume 56. P. 93–102.
2. Barral V., Suárez-Casal P., Escudero C.J., García-Naya J.A. Multi-Sensor Accurate Forklift Location and Tracking Simulation in Industrial Indoor Environments. *Electronics*. 2019. Volume 8(10). P. 1152. <https://doi.org/10.3390/electronics8101152>.
3. Binyam Shiferaw Heyi, Implementation of Indoor Positioning using IEEE802.15.4a (UWB). A Thesis submitted for partial fulfillment of the Masters of Science in Electrical Engineering Major in Network Services And Systems (Stockholm, Sweden January, 2013).
4. Moshenskyi, A., Novak, D., Oleshchenko, L. (2023). Sub-Gigahertz Wireless Sensor Network for Smart Clothes Monitoring. In: Hu, Z., Dychka, I., He, M. (eds) *Advances in Computer Science for Engineering and Education VI. ICCSEE 2023. Lecture Notes on Data Engineering and Communications Technologies*, vol 181. Springer, Cham. https://doi.org/10.1007/978-3-031-36118-0_59.
5. Moshenskyi A. Private rescue echo beacon with FSK radiomodule. *Scientific journal "Science-Based Technologies"*, 4(48), 2020, pp. 478-483.
6. Mohsen Salehi, Jamal Karimian. A Trust-based Security Approach in Hierarchical Wireless Sensor Networks. *International Journal of Wireless and Microwave Technologies(IJWMT)*, Vol.7,No.6, pp. 58-67, 2017.

МЕТОДИ ЗАХИСТУ ВІД АТАК НА ОДНОРАНГОВІ БЛОКЧЕЙН МЕРЕЖІ БІТКОІНА

Валуйський С.В., Кравчук І.В.

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна
E-mail: ilyukha.kravchuk@gmail.com*

METHODS OF PROTECTION AGAINST ATTACKS ON PEER- TO-PEER BLOCKCHAIN NETWORKS OF BITCOIN

This work is focused on researching and developing methods to protect against attacks on the peer-to-peer blockchain network of Bitcoin. This will involve analyzing various types of attacks and developing and implementing new security methods, such as multisignatures, confidential transactions, enhanced authentication, and smart contracts.

Біткоїн був запропонований у 2008 році під псевдонімом Сатоші Накамото через документ, опублікований на криптографічному форумі. У січні 2009 року відбулася перша транзакція біткоїну між Накамото та розробником Галеном Філдсом. Біткоїн став першою криптовалютою, яка використовує технологію блокчейн для забезпечення децентралізованого обміну валюти. З 2010 року біткоїн став предметом значного інтересу як серед технологічно орієнтованих груп, так і серед інвесторів.

Біткоїн має однорангову блокчейн мережу, де кожен вузол має однакові права та можливості. Кожен вузол може виступати як клієнт, що ініціює транзакції, так і сервер, що обробляє та передає їх. Мережа функціонує без централізованого органу контролю чи управління, кожен вузол має копію блокчейну, що містить історію всіх транзакцій.

Ключовим елементом мережі є процес майнінгу, де спеціалізовані комп'ютери (майнери) розв'язують складні математичні завдання для підтвердження та обробки транзакцій. Цей процес забезпечує безпеку та надійність мережі, додаючи нові блоки з транзакціями до блокчейну. Однорангова структура мережі дозволяє біткоїну працювати без централізованої влади чи контролю, забезпечуючи при цьому високий рівень безпеки та анонімності. Кожен учасник мережі може бачити та перевіряти всі транзакції, забезпечуючи прозорість та відкритість системи.

Мета роботи. Основна мета роботи полягає в дослідженні методів захисту від атак на однорангові блокчейн мережі біткоїна. Для цього використовуються аналіз різних видів атак, таких як повторна витрата, атака 51%, форкінг та селфіш-майнінг, а також розробка та аналіз ефективних методів захисту від них.

Огляд методів захисту від атак на однорангові блокчейні мереж [1-4].

Multisig. Використання мультипідписів дозволяє створювати адреси, які потребують авторизації від кількох підписників для здійснення транзакції. Це

підвищує безпеку та зменшує ризик втрати коштів внаслідок несанкціонованих транзакцій.

Confidential Transactions. Використання криптографічних протоколів, які дозволяють захистити конфіденційність суми транзакцій, забезпечуючи при цьому можливість перевірки їх валідності (рис.1).

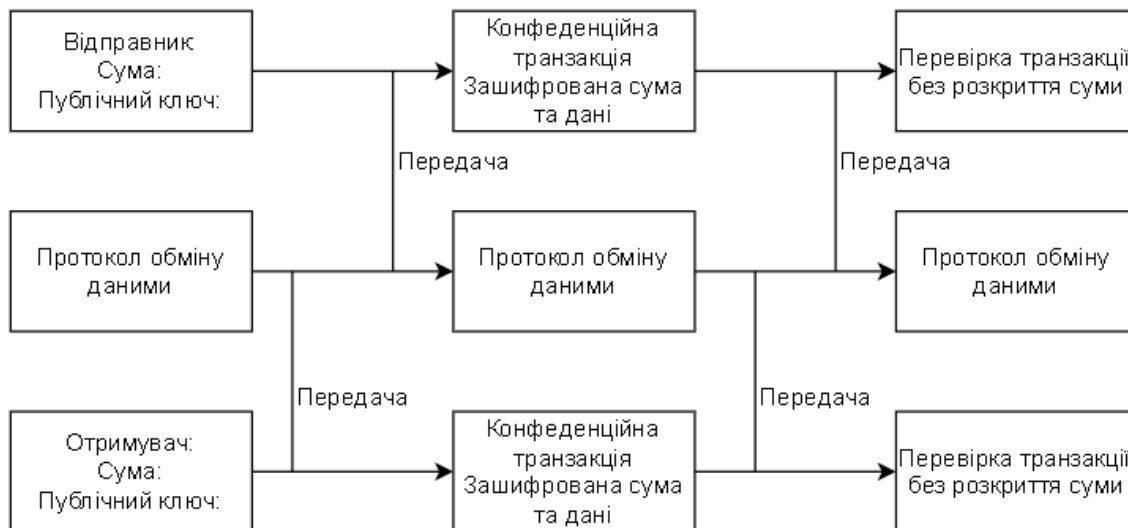


Рис.1. Приклад роботи Confidential Transactions.

Enhanced Authentication Schemes. Розробка та впровадження методів аутентифікації, які базуються на більш складних криптографічних протоколах, що ускладнюють спроби підробки транзакцій (рис.2).

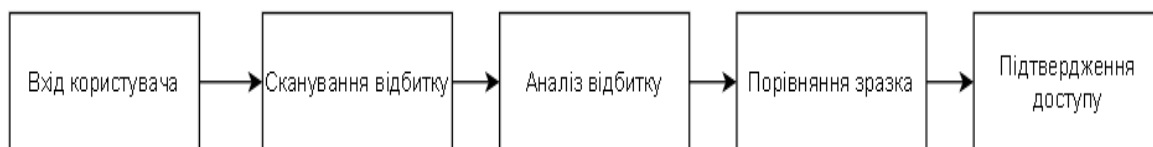


Рис.2. Приклад Enhanced Authentication Schemes (біометричної аутентифікації).

Smart Contracts. Розробка смарт-контрактів для автоматизації та забезпечення безпеки операцій, що відбуваються в мережі біткоїна, таких як умовні операції або розподіл коштів в залежності від виконання певних умов.

Взаємодія між відправником та отримувачем полягає в обміні зашифрованими даними та доказами через спеціальний протокол обміну. Цей протокол дозволяє їм здійснювати конфіденційну транзакцію, зберігаючи приватність сум, які не розкриваються сторонами під час процесу обміну.

Біометрична аутентифікація для користувача біткоїна включає сканування відбитка пальця, його аналіз для визначення унікальних характеристик, порівняння з зразком у системі і, в разі підтвердження відповідності, надання доступу до біткоїн-гаманця або функціоналу.

Smart Contracts спочатку створюються, після чого визначаються їх умови, включаючи параметри та обмеження (рис.3). Умови зберігаються, і потім виконуються, перевіряючи їх на виконання та виконуючи відповідні дії в залежності від результатів.

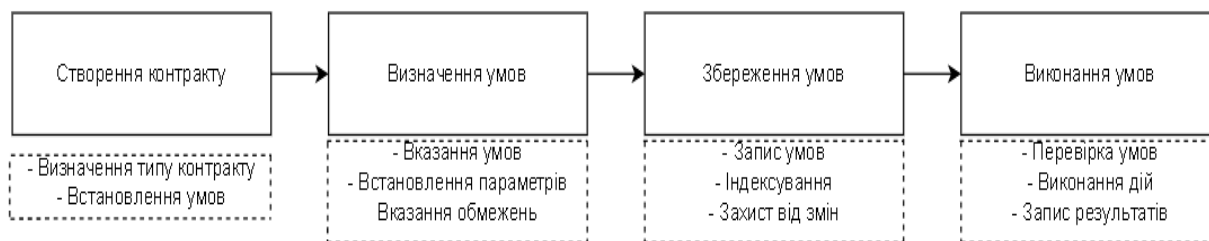


Рис.3. Smart Contracts

Висновок. Робота спрямована на розробку та аналіз ефективних методів захисту від цих атак. Досліджуючи методи захисту, розглянуто такі методи, як Multisig, Confidential Transactions, Enhanced Authentication Schemes та Smart Contracts. Multisig дозволяє створювати адреси, які потребують авторизації від кількох підписників для здійснення транзакцій, підвищуючи при цьому безпеку. Confidential Transactions забезпечують захист конфіденційності сум транзакцій, а Enhanced Authentication Schemes ускладнюють спроби підробки транзакцій за допомогою складних криптографічних протоколів. Smart Contracts автоматизують та забезпечують безпеку операцій, що відбуваються в мережі біткоїна, виконуючи умовні операції згідно з певними параметрами.

Література

1. Bitcoin's Blockchain Peer-to-Peer Network Security Attacks and Countermeasures / Mahmoud Mostafa. INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY, february 2020, Vol 13(07), 767 – 786. URL: <https://doi.org/10.17485/ijst/2020/v13i07/149691>.
2. Refund Attacks on Bitcoin's Payment Protocol / McCorry Patrick, Shahandashti Siamak F. Financial Cryptography and Data Security, 22-26 Feb 2016. URL: https://doi.org/10.1007/978-3-662-54970-4_34.
3. Formal Modelling and Security Analysis of Bitcoin's Payment Protocol / Paolo Modesti, Siamak F. Shahandashti, Patrick McCorry, Feng Hao. Computers & Security, Volume 107, 2021, 102279, ISSN 0167-4048, URL: <https://doi.org/10.1016/j.cose.2021.102279>.
4. An enhanced authentication scheme for Internet of Things and cloud based on elliptic curve cryptography / Pallavi Bhuarya, Preeti Chandrakar, Rifaqat Ali, Aakanksha Sharaff. Communication systems, Volume 34, Issue 10, 10 July 2021. URL: <https://doi.org/10.1002/dac.4834>.

МЕТОДИ КЛАСТЕРИЗАЦІЇ В БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ НАСТУПНОГО ПОКОЛІННЯ

Валуйський С.В., Кисіль А.І.

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна
E-mail: valuisnyi.stanislav@lll.kpi.ua*

CLUSTERING METHODS IN NEXT-GENERATION WIRELESS SENSOR NETWORKS

Wireless Sensor Networks (WSNs) are vital for diverse applications, but their efficiency relies heavily on clustering methods. This review delves into the latest innovations in clustering for next-gen WSNs, emphasizing energy efficiency, scalability, adaptability, load balancing, security, and node heterogeneity. By addressing these factors, modern clustering techniques aim to prolong network lifespan, optimize data transmission, and ensure robust performance. This overview provides valuable insights for researchers and practitioners in wireless communications and sensor networks.

Кластеризація в безпроводових сенсорних мережах наступного покоління є важливим завданням для оптимізації роботи таких мереж. Основна мета кластеризації полягає в групуванні вузлів мережі в кластери з метою підвищення ефективності комунікації, зменшення споживання енергії та підвищення довговічності мережі. Наступне покоління безпроводових сенсорних мереж може використовувати різноманітні методи кластеризації, включаючи класичні підходи, такі як алгоритми K-Means або агломеративну кластеризацію, а також спеціалізовані методи, розроблені спеціально для безпроводових сенсорних мереж.

Деякі з основних методів кластеризації в безпроводових сенсорних мережах наступного покоління включають:

1. LEACH (Low Energy Adaptive Clustering Hierarchy): Це один з найпопулярніших протоколів кластеризації в безпроводових сенсорних мережах. LEACH розроблений для зменшення споживання енергії, розподілу навантаження та підвищення довговічності мережі.

2. SEP (Stable Election Protocol): Цей протокол базується на ідеї вибору стійких (стабільних) вузлів кластеру в якості головних вузлів (cluster head). Це допомагає підвищити стійкість та продовжити життєвий цикл мережі.

3. TEEN (Threshold sensitive Energy Efficient sensor Network protocol): Цей протокол зосереджений на підвищенні енергоефективності мережі шляхом визначення порогових значень для вимірюваних параметрів, таких як температура чи освітленість.

4. HEED (Hybrid Energy-Efficient Distributed clustering): HEED комбінує ідеї кластеризації та енергоефективності для покращення роботи безпроводових сенсорних мереж. Протокол спрямований на збалансування навантаження та енергозбереження.

5. PEGASIS (Power-Efficient Gathering in Sensor Information Systems): Цей протокол використовує ланцюгову топологію для передачі даних від датчиків до базової станції, максимізуючи енергоефективність і подовжуючи час життя мережі.

Ці методи використовуються для оптимізації функціонування безпроводових сенсорних мереж наступного покоління, забезпечуючи більш ефективну комунікацію та зменшуючи споживання енергії.

Звичайні задачі кластеризації в безпроводових сенсорних мережах включають розподіл вузлів на кластери, вибір кластерних головних вузлів (cluster heads), оптимізацію передачі даних між вузлами та кластерними головами, управління енергією, забезпечення безпеки даних тощо.

Крім того, деякі інноваційні підходи до кластеризації включають в себе використання штучного інтелекту та машинного навчання для покращення ефективності кластеризації та управління мережею. Наприклад, можливе використання алгоритмів навчання з підкріпленням для динамічного вибору кластерних головних вузлів залежно від змінюючихся умов мережі.

Однією з ключових проблем, які вирішуються в цьому контексті, є балансування навантаження між кластерними головними вузлами, щоб уникнути перевантаження деяких вузлів та недоексплуатації інших. Також важливо враховувати змінні умови мережі, такі як зміни в енергопостачанні, обмеження на рухомість вузлів та зміни у трафіку даних.

Наступне покоління безпроводових сенсорних мереж також може використовувати технології мережевого вирішення проблем, такі як blockchain, для забезпечення безпеки, конфіденційності та інтегритету даних, що пересилаються в мережі.

Додаткові аспекти, які слід врахувати в контексті кластеризації в безпроводових сенсорних мережах наступного покоління, включають:

1. Мобільність вузлів: У деяких застосуваннях вузли можуть бути мобільними, що може вплинути на кластеризацію та маршрутизацію даних. Кластерні структури можуть потребувати постійного оновлення через переміщення вузлів.

2. Гетерогенність вузлів: Безпроводові сенсорні мережі можуть включати в себе вузли з різною обчислювальною потужністю, дальністю передачі, сенсорними можливостями тощо. Ефективна кластеризація повинна враховувати цю гетерогенність.

3. Розділення задач (task partitioning): У деяких застосуваннях мережі можуть бути задіяні для виконання різних завдань. Кластеризація може бути оптимізована для ефективного розподілу цих задач між вузлами.

4. Безпека даних: Оскільки безпроводові сенсорні мережі часто використовуються для збирання чутливих даних, важливо забезпечити захист цих даних від несанкціонованого доступу. Кластеризація може впливати на механізми безпеки даних в мережі.

5. Масштабованість: Застосування може вимагати масштабування мережі великої кількості вузлів. Ефективна кластеризація повинна бути здатна працювати в умовах великої кількості вузлів без втрати

продуктивності.

Ці аспекти демонструють складність завдання кластеризації в безпроводових сенсорних мережах наступного покоління та необхідність розробки розумних та адаптивних алгоритмів для оптимізації функціонування таких мереж.

Особливості методів кластеризації в безпроводових сенсорних мережах наступного покоління включають:

1. Енергоефективність: Основна увага при розробці методів кластеризації спрямована на збереження енергії вузлів мережі, оскільки вони часто живуть в обмежених умовах живлення. Методи кластеризації повинні оптимізувати розподіл навантаження та енергопотребу вузлів, забезпечуючи максимальну довговічність мережі.

2. Скалабельність: Завдяки швидкому росту кількості підключених пристроїв у безпроводових сенсорних мережах, методи кластеризації повинні бути здатні працювати ефективно в умовах великого обсягу даних та великої кількості вузлів.

3. Динамічність: Методи кластеризації повинні бути адаптивними до змінних умов мережі, таких як рухомість вузлів, зміна трафіку даних, а також втрати зв'язку.

4. Балансування навантаження: Ефективні методи кластеризації повинні забезпечувати рівномірне розподіл навантаження між кластерними головними вузлами, запобігаючи перевантаженню деяких вузлів та підвищуючи загальну продуктивність мережі.

5. Безпека: Методи кластеризації повинні враховувати аспекти безпеки, такі як захист від атак, конфіденційність даних та аутентифікація вузлів, щоб забезпечити безпеку даних у безпроводових сенсорних мережах.

6. Врахування гетерогенності: Методи кластеризації повинні бути здатні працювати з різними типами вузлів та різними характеристиками, такими як обчислювальна потужність, дальність передачі даних та сенсорні можливості.

Врахування цих особливостей допомагає розробити ефективні та надійні методи кластеризації для безпроводових сенсорних мереж наступного покоління.

Література

1. Heinzelman, Wendi B., Anantha P. Chandrakasan, and Hari Balakrishnan. "Energy-efficient communication protocol for wireless microsensor networks." Proceedings of the 33rd annual Hawaii international conference on system sciences. 2000.
2. Lindsey, Scott, and Cauligi S. Raghavendra. "PEGASIS: Power-efficient gathering in sensor information systems." Aerospace conference proceedings, 2002. IEEE, 2002.
3. Manjeshwar, Arati, and Dharma P. Agrawal. "TEEN: a routing protocol for enhanced efficiency in wireless sensor networks." Distributed Computing Systems Workshops, 2001. Proceedings. 2001 International Conference on. IEEE, 2001.
4. Abbasi, Abdul R., and Mohamed Younis. "A survey on clustering algorithms for wireless sensor networks." Computer communications 30.14-15 (2007): 2826-2841.
5. Yu, Honghai, et al. "LEACH-C: A clustering protocol for wireless sensor networks." Sensors 9.5 (2009): 3800-3817.



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

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ
НДІ ТЕЛЕКОМУНІКАЦІЙ**

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

17-18 квітня 2024 року

Тези конференції

м. Київ

ПРОГРАМНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ ПРІТС-2024

Співголови конференції:

- 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;
- ЯКОРНОВ Є.А. – к.т.н., професор Навчально-наукового Інституту телекомунікаційних систем КПІ ім. Ігоря Сікорського;
- КРАВЧУК І.М. – к.ю.н., доц., Навчально-наукового Інституту телекомунікаційних систем КПІ ім. Ігоря Сікорського;
- КОСОГОР А.В. – в.о. голови студради 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., проф., КПІ ім. Ігоря Сікорського, Київ;
- МОШИНСЬКА А.В. - д.т.н., доц., 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.
- МАКСИМОВ В.В. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ;
- МІНОЧКІН Д.А. - к.т.н., доц., КПІ ім. Ігоря Сікорського, Київ.

Члени програмного комітету:

- Авдеєнко Г.Л., к.т.н., в.о. директора НН ІТС, КПІ ім. Ігоря Сікорського, НН ІТС, Київ;
- Валуйський С.В., к.т.н., доц., КПІ ім. Ігоря Сікорського, НН ІТС, Київ;
- Курдеча В.В., ст. викладач, КПІ ім. Ігоря Сікорського, НН ІТС, Київ;
- Новіков В.І., к.т.н., ст. викладач, КПІ ім. Ігоря Сікорського, НН ІТС, Київ.

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

**SMART КАЛЕНДАР ДЛЯ ІОТ ПРИЛАДІВ
НА ПРИКЛАДІ ТЕХНОЛОГІЇ MATTER**

Муха Р.В.

Науковий керівник: **Токар Л.О.**

*Харківський національний університет радіоелектроніки,
кафедра ІКІ ім.В.В.Поповського, Україна
E-mail: rostyslav.mukha@nure.ua*

Дослідження принципів роботи протоколів, таких як Wi-Fi, Zigbee, Z-Wave та Thread, з метою вивчення їхніх характеристик та аналізу способів уніфікації. Особлива увага приділяється передовій технології Matter, яка визначає нові стандарти взаємодії між різноманітними пристроями розумного будинку, сприяючи створенню єдиної та оптимізованої мережі для користувача.

Аналіз та використання Google Calendar API як основного інструменту для реалізації SMART календаря. Опис принципів роботи API та його інтеграції зі створюваною системою.

**SMART CALENDAR FOR IOT DEVICES,
ON THE EXEMPLE OF MATTER TECHNOLOGY**

Mukha R.V.

Scientific adviser: **Tokar L.O.**

*Kharkiv National University of Radio Electronics,
Department of ICT named after V.V. Popovsky, Ukraine
E-mail: rostyslav.mukha@nure.ua*

Explore the principles of protocols such as Wi-Fi, Zigbee, Z-Wave, and Thread to learn their characteristics and analyze how to unify them. Particular attention is paid to the advanced Matter technology, which defines new standards for interaction between various smart home devices, contributing to the creation of a unified and optimized network for the user.

Analysis and use of the Google Calendar API as the main tool for implementing a SMART calendar. Description of the principles of API operation and its integration with the system under development.

КЛАСТЕРИЗАЦІЯ В МЕРЕЖАХ VANET

Соловйов П.В.

Науковий керівник: **Токар Л.О.**

*Харківський національний університет радіоелектроніки,
кафедра ІКТ ім. В.В.Поповського, Україна*

E-mail: pavlo.soloviov@nure.ua

Це дослідження детально аналізує методи кластеризації в мережах VANET, метою яких є покращення ефективності передавання даних та управління мережею.

У роботі розглядаються різні алгоритми формування кластерів, досліджується їхній вплив на ключові параметри мережі, такі як пропускна спроможність і час затримки передачі інформації.

Особливо підкреслюється значення адаптивних стратегій управління кластерами, які дозволяють мережі ефективно реагувати на умови, що змінюються в динамічному дорожньому середовищі.

У роботі виявляються основні труднощі, з якими стикаються розробники під час реалізації кластеризації у VANET, і пропонуються можливі шляхи їх вирішення. Додатково акцентується увага на значенні кластеризації для інтеграції VANET в інтелектуальні транспортні системи, що відкриває нові перспективи для підвищення безпеки та ефективності на дорогах.

CLUSTERING IN VANET NETWORKS

Soloviov P.V.

Scientific adviser: **Tokar L.O.**

*Kharkiv National University of Radio Electronics,
Department of ICT named after V.V. Popovsky, Ukraine*

E-mail: pavlo.soloviov@nure.ua

This research provides a detailed analysis of clustering techniques in VANET networks, which aim to improve the efficiency of data transmission and network management.

The paper reviews different cluster formation algorithms and investigates their impact on key network parameters such as throughput and information transmission delay time.

The importance of adaptive cluster management strategies is particularly emphasized, which enable the network to respond effectively to changing conditions in a dynamic traffic environment.

The paper identifies the main challenges faced by developers in implementing clustering in VANETs and suggests possible solutions. Additionally, the importance of clustering for integrating VANETs into intelligent transportation systems is emphasized, which opens new perspectives for improving safety and efficiency on roads.

АНАЛІЗ МАТЕМАТИЧНИХ МОДЕЛЕЙ МАРШРУТИЗАЦІЇ ТА ЇХ ЗАСТОСУВАННЯ В ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖАХ

Лемешко В.О., Персіков М.А.

Науковий керівник: **Єременко О.С.**

Харківський національний університет радіоелектроніки, Україна

E-mail: valentyn.lemeshko@nure.ua, mykhailo.persikov@nure.ua

Досліджено процеси маршрутизації, що відіграють провідну роль під час вирішення завдань забезпечення якості обслуговування, надійності та мережної безпеки в програмно-конфігурованих мережах. Доведено, що гідною альтернативою графовим моделям є використання потокових моделей маршрутизації. Хоча потокові та графові моделі адекватно враховують зміни у стані мережі та забезпечують пошук оптимального рішення, потокові моделі враховують характеристики потоків пакетів, що передаються. Крім того, за необхідності в межах потокових моделей є можливість максимізувати або мінімізувати один з показників якості обслуговування, надійності або мережної безпеки.

ANALYSIS OF MATHEMATICAL ROUTING MODELS AND THEIR APPLICATION IN SOFTWARE-DEFINED NETWORKS

Lemeshko V.O., Persikov M.A.

Scientific adviser: **Yeremenko O.S.**

Kharkiv National University of Radio Electronics, Ukraine

E-mail: valentyn.lemeshko@nure.ua, mykhailo.persikov@nure.ua

The study investigates the routing processes that play a leading role in solving the problems of ensuring the Quality of Service, reliability, and network security in the Software-Defined Networks. It is proved that a worthy alternative to graph models is the application of flow-based routing models. Although flow-based and graph models adequately consider changes in the network state and provide a search for an optimal solution, flow-based models take into account the characteristics of packet flows. In addition, if necessary, flow-based models have the ability to maximize or minimize one of the following indicators of the Quality of Service, reliability, or network security.

ДОСЛІДЖЕННЯ МОДЕЛЕЙ МАРШРУТИЗАЦІЇ ІЗ ЗАБЕЗПЕЧЕННЯМ НАДІЙНОСТІ ТА ВІДМОВОСТІЙКОСТІ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Солом'яний М.В., Персіков М.А.

Науковий керівник: Єременко О.С.

Харківський національний університет радіоелектроніки, Україна

E-mail: maksym.solomianyi@nure.ua, mykhailo.persikov@nure.ua

Досліджено технології та засоби забезпечення якості обслуговування, надійності та відмовостійкості в інфокомунікаційних мережах. Визначено особливості гарантування міжкінцевої надійності та відмовостійкості в мережах засобами маршрутизації, де також приділено увагу реалізації високої доступності. Розглянуто поняття та класифікацію моделей маршрутизації щодо забезпечення міжкінцевої якості обслуговування та відмовостійкості. Проведено дослідження потокової моделі надійної маршрутизації. Для цього описано базову потокову модель маршрутизації для одношляхової та багатошляхової стратегій, а також проведено моделювання та аналіз ефективності моделі надійної маршрутизації.

STUDY OF ROUTING MODELS WITH RELIABILITY AND FAULT TOLERANCE IN INFORMATION AND COMMUNICATION NETWORKS

Solomianyi M.V., Persikov M.A.

Scientific adviser: Yeremenko O.S.

Kharkiv National University of Radio Electronics, Ukraine

E-mail: maksym.solomianyi@nure.ua, mykhailo.persikov@nure.ua

Technologies and means of ensuring the Quality of Service, reliability, and fault tolerance in infocommunication networks are investigated. The peculiarities of guaranteeing end-to-end reliability and fault tolerance in networks employing routing are determined, where attention is paid to implementing high availability. The concept and classification of routing models ensure end-to-end Quality of Service and fault tolerance are examined. A study of the flow-based model of availability-aware routing is carried out. For this purpose, the basic flow-based model of routing for single-path and multipath strategies is described, and the simulation and analysis of the effectiveness of the availability-aware routing model are conducted.

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ВІДМОВСТІЙКОСТІ ЗАСОБАМИ МАРШРУТИЗАЦІЇ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Недоступ Д.М., Персіков М.А.

Науковий керівник: **Єременко О.С.**

Харківський національний університет радіоелектроніки, Україна

E-mail: daniil.nedostup@nure.ua, mykhailo.persikov@nure.ua

Досліджено сучасні підходи, моделі, методи та алгоритми, за допомогою яких вирішується проблема забезпечення відмовостійкості інфокомунікаційних мереж. Особливу увагу приділено методам відмовостійкої маршрутизації як ефективним засобам забезпечення стійкості мереж до внутрішніх і зовнішніх факторів. Розв'язано задачу відмовостійкої маршрутизації на основі математичних потокових моделей швидкої перемаршрутизації з використанням схем резервування каналу та вузла. Проведено дослідження та порівняльний аналіз побудови маршрутних рішень для основного та резервного шляхів за умови багатопляхової стратегії маршрутизації та різних метрик по аналогії з протоколами RIP та OSPF.

RESEARCH OF FAULT-TOLERANCE METHODS BY ROUTING MEANS IN INFOCOMMUNICATION NETWORKS

Nedostup D.M., Persikov M.A.

Scientific adviser: **Yeremenko O.S.**

Kharkiv National University of Radio Electronics, Ukraine

E-mail: daniil.nedostup@nure.ua, mykhailo.persikov@nure.ua

Modern approaches, models, methods, and algorithms that solve the problem of ensuring the fault tolerance of information and communication networks are investigated. Particular attention is paid to fault-tolerant routing methods as an effective means of ensuring the network's resilience to internal and external factors. The problem of fault-tolerant routing is solved based on mathematical flow-based models of fast rerouting using link and node redundancy schemes. A study and comparative analysis of the routing solutions construction for the primary and backup paths under the condition of a multipath routing strategy and various metrics by analogy with the RIP and OSPF protocols are carried out.

ДОСЛІДЖЕННЯ ПРОЦЕСУ БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ ДЛЯ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ МЕРЕЖ З ВИКОРИСТАННЯМ ПРОАКТИВНИХ І РЕАКТИВНИХ ПІДХОДІВ

Персіков А.В., Шестопапов С.С.

Науковий керівник: **Єременко О.С.**

*Харківський національний університет радіоелектроніки, Україна
E-mail: anatolii.persikov@nure.ua, serhii.shestopalov@protonmail.com*

Проведено аналіз специфікацій та рекомендацій щодо розробки кіберстійких систем, а також особливостей інженерії кіберстійкості як спеціальної дисципліни системної інженерії, що застосовується разом з інженерією безпеки систем та інженерією стійкості для розробки живучих, надійних і безпечних інфокомунікаційних систем. Виконано аналіз і класифікацію загроз мережного рівня, а також можливостей засобів маршрутизації для забезпечення безпеки та стійкості мереж. Зосереджено увагу на проактивних і реактивних підходах щодо безпечної маршрутизації. Досліджено обрані моделі вимовостійкої безпечної маршрутизації на основі показників компрометації елементів мережі.

INVESTIGATION OF THE SECURE ROUTING PROCESS TO ENSURE NETWORK RESILIENCE USING PROACTIVE AND REACTIVE APPROACHES

Persikov A.V., Shestopalov S.S.

Scientific adviser: **Yeremenko O.S.**

*Kharkiv National University of Radio Electronics, Ukraine
E-mail: anatolii.persikov@nure.ua, serhii.shestopalov@protonmail.com*

The work analyses the specifications and recommendations for developing cyber-resilient systems, as well as the features of cyber resilience engineering as a special discipline of systems engineering, which is used together with systems security engineering and resilience engineering to develop survivable, reliable, and secure information and communication systems. The study analyses and classifies network layer threats and routing tools' capabilities to ensure network security and resilience. Attention is focused on proactive and reactive approaches to secure routing. The selected models of fault-tolerant secure routing based on the indicators of network elements compromise are investigated.

ВИКОРИСТАННЯ МЕТОДІВ ШТУЧНОГО ІНТЕЛЕКТУ ПІД ЧАС РОЗВ'ЯЗАННЯ ЗАДАЧ ОПТИМІЗАЦІЇ ЯКОСТІ ОБСЛУГОВУВАННЯ В МЕРЕЖАХ 6G

Скомаха М. О.

Науковий керівник: **Єременко О.С.**

Харківський національний університет радіоелектроніки, Україна

E-mail: mykyta.skomakha@nure.ua

Проведено аналіз і класифікацію методів штучного інтелекту (ШІ) та їх роль в оптимізаційних операціях у мобільних мережах шостого покоління – 6G. Для дослідження обрано моделі самонавчання ШІ, а саме машинне та глибоке навчання. Разом з тим проведено їх порівняння. Розглянуто такі методи, як федеративне, з підсиленням, кероване та некероване навчання, а також завдання оптимізації якості обслуговування, що вони можуть вирішувати. На основі аналізу визначено перспективність і потенційну ефективність застосування ШІ щодо оптимізації в мережах 6G, адже такий підхід використовуватиме дані та контекст для навчання та вдосконалення рішень, що дозволить адаптуватися до динамічних умов мережі та змінних потреб користувачів.

THE APPLICATION OF ARTIFICIAL INTELLIGENCE METHODS IN SOLVING QUALITY OF SERVICE OPTIMIZATION PROBLEMS IN 6G NETWORKS

Skomakha M.O.

Scientific adviser: **Yeremenko O.S.**

Kharkiv National University of Radio Electronics, Ukraine

E-mail: mykyta.skomakha@nure.ua

The study analyzes and classifies artificial intelligence (AI) methods and their role in optimizing operations in sixth-generation mobile networks (6G). The AI self-learning models, namely machine learning and deep learning, were selected for the study. At the same time, their comparison is carried out. The work considers such methods as federated, reinforcement learning, supervised and unsupervised learning, as well as the Quality of Service optimization tasks that they can solve. Based on the analysis, AI's prospects and potential effectiveness for optimization in 6G networks are determined since this approach will use data and context to learn and improve solutions, which will allow adapting to dynamic network conditions and changing user needs.

АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ЗБОРУ ІНФОРМАЦІЇ ВУЗЛІВ ІНТЕРНЕТУ РЕЧЕЙ

Солоденко М.А.

Науковий керівник: **Курдеча В.В.**

Навчально-науковий інститут телекомунікаційних

систем КПІ ім. Ігоря Сікорського, Україна

E-mail: mushenok.mariia@iit.kpi.ua

Стрімке зростання кількості пристроїв Інтернету речей призвело до появи потреби в нових методах збору інформації. В даній роботі досліджено переваги та недоліки технології Інтернету речей, проаналізовано існуючі методи, моделі та засоби збору інформації вузлів IoT з застосуванням стільникових мереж, виділено загальні етапи та вимоги до збору та обробки даних.

ANALYSIS OF EXISTING METHODS OF COLLECTING INFORMATION FROM IoT NODES

Solodenko M.A.

Scientific adviser: **Kurdecha V.V.**

Educational and Scientific Institute of Telecommunication

Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: mushenok.mariia@iit.kpi.ua

The dynamic growth number of IoT devices has led to the need for new methods of data collection. This report explores the advantages and disadvantages of IoT technology, analyses existing methods, models, and tools for collecting information from IoT nodes using cellular networks, identifies general stages and requirements for data collection and processing.

ОСОБЛИВОСТІ ОНОВЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В ПРИСТРОЯХ ІНТЕРНЕТУ РЕЧЕЙ

Терещенко В.О.

Науковий керівник: **Курдеча В.В.**

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна
E-mail: tereshenkovladislavovich2312@gmail.com*

Досліджено важливість оновлення програмного забезпечення в інтернеті речей через ризики виходу пристроїв з ладу. Аналіз вказує на людський фактор як основну причину виходу з ладу, оскільки з розвитком технологій з'являються нові вразливості. Запропоновано різні методи оновлення, доступні як для виробників, так і для звичайних користувачів, такі як OTA, LAN та USB, а також методи, які вимагають спеціалізованого підходу, наприклад, використання власних роз'ємів, пряме дротове підключення чи заміна частини пристрою що відповідає за операційну систему.

FEATURES OF SOFTWARE UPDATE IN INTERNET OF THINGS DEVICES

Tereshchenko V.O.

Scientific adviser: **Kurdecha V.V.**

*Educational and Scientific Institute of Telecommunication
Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: tereshenkovladislavovich2312@gmail.com*

The importance of software updates in the Internet of Things due to the risks of device failure has been investigated. The analysis points to the human factor as the main cause of failure, as new vulnerabilities appear with the development of technology. Various update methods are offered, available to both manufacturers and ordinary users, such as OTA, LAN and USB, as well as methods that require a specialized approach, such as using proprietary connectors, direct wired connection or replacing a part of the device that corresponds for the operating system.

МОЖЛИВОСТІ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ НА ФІЗИЧНОМУ РІВНІ У ТЕЛЕКОМУНІКАЦІЯХ

Радуга Н.С. Прудкий В.С.

Науковий керівник: **Курдеча В.В.**

Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: raduganazar@gmail.com, reker166@gmail.com

Ця робота розглядає можливості застосування технологій штучного інтелекту на фізичному рівні у телекомунікаціях. Досліджується, як алгоритми машинного навчання можуть оптимізувати роботу мережі, підвищуючи її ефективність та стійкість до перешкод. Зокрема, розглядаються можливості застосування нейромереж для прогнозування навантаження на мережу, автоматичного виявлення та усунення несправностей, а також оптимізації маршрутизації даних з метою зниження затримок і підвищення пропускної здатності.

POSSIBILITIES OF APPLICATION OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN TELECOMMUNICATIONS

Raduga N.S. Prudkyi V.S.

Scientific adviser: **Kurdecha V.V.**

Educational and Scientific Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: raduganazar@gmail.com, reker166@gmail.com

This work considers the possibilities of using artificial intelligence technologies at the physical level in telecommunications. The study reveals how machine learning algorithms can optimize network performance, increasing its efficiency and resistance to interference. In particular, the possibilities of using neural networks for predicting network load, automatic detection and elimination of faults, as well as optimization of data routing in order to reduce delays and increase throughput are discussed.

ВПЛИВ СОЦІАЛЬНИХ МЕДІА НА СПРИЙНЯТТЯ ІНФОРМАЦІЇ

Пінчук Ю.М.

Науковий керівник: **Курдеча В.В.**

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна*

E-mail: pinchuk.yulia@lil.kpi.ua

Досліджено тему впливу соціальних медіа на сприйняття інформації. Визначення поняття «соціальні медіа». Висвітлена актуальність проблеми, її роль у сучасному інформаційному суспільстві. Наведена статистика користування соціальними медіа, короткий аналіз показників використання популярних платформ. Представлений прогноз розвитку тенденцій використання соціальних медіа. Показано декілька аспектів проблематики та виокремлено проблему дезінформації і більш детально її розглянуто. Наведені рекомендації з медіаграмотності, пропозиції як збільшити рівень освіченості користувачів соціальних медіа і покращити навички для розпізнавання дезінформації та критичного мислення в мережі.

SOCIAL MEDIA'S IMPACT ON THE PERCEPTION OF INFORMATION

Pinchuk Y.M.

Scientific adviser: **Kurdecha V.V.**

*Educational and Scientific Institute of Telecommunication
Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine*

E-mail pinchuk.yulia@lil.kpi.ua

The influence of social media on the perception of information has been studied. Definition of the term "social media". The problem's relevance and role in the modern information society is highlighted. The statistics of the use of social media are given, as well as a brief analysis of the indicators of the use of popular platforms. The forecast of the development of trends in the use of social media is presented. Several aspects of the problem are shown and the problem of disinformation is singled out and considered in more detail. Recommendations for media literacy, suggestions for increasing the level of education of social media users, and improving skills for recognizing misinformation and critical thinking in the network are given.

ТЕНДЕНЦІЇ РОЗВИТКУ ОПТОВОЛОКОННИХ ТЕХНОЛОГІЙ

Бех В.О., Касіч Н.Ю.

Науковий керівник: **Курдеча В.В.**

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна*

E-mail: behv31316@gmail.com; kasich.nszar@gmail.com

Тема розвитку оптоволоконних технологій є актуальною через їх широке використання у різних галузях, таких як телекомунікації, медицина, виробництво та інші. Розвиток оптоволоконних технологій дозволяє поліпшити передачу даних, зменшити витрати і підвищити ефективність мереж зв'язку. Робота аналізує інноваційні технології, вирішує технічні проблеми та висуває рекомендації для подальшого розвитку оптоволоконних систем, спрямовані на поліпшення їх функціональності та доступності для різних сфер застосування. На основі проведеного аналізу висунуто рекомендації щодо подальшого розвитку оптоволоконних технологій, включаючи можливі напрямки досліджень та інновацій.

TRENDS IN THE DEVELOPMENT OF FIBER OPTIC TECHNOLOGIES

Bekh V.O., Kasich N.Y.

Scientific adviser: **Kurdecha V.V.**

*Educational and Scientific Institute of Telecommunication
Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine*

E-mail: behv31316@gmail.com; kasich.nszar@gmail.com

The development of fiber optic technologies is relevant due to their wide usage in various sectors such as telecommunications, medicine, manufacturing, and others. The advancement of fiber optic technologies enables the enhancement of data transmission, reduction of costs, and improvement in the efficiency of communication networks. This paper analyzes innovative technologies, addresses technical challenges, and provides recommendations for the further development of fiber optic systems aimed at improving their functionality and accessibility across different application domains. Based on the conducted analysis, recommendations for the future development of fiber optic technologies are proposed, including potential research directions and innovations.

БЕЗДРОТОВІ ТЕХНОЛОГІЇ ПЕРЕДАЧІ ДАНИХ НА ВЕЛИКІ ВІДСТАНІ В МЕРЕЖАХ ІНТЕРНЕТУ РЕЧЕЙ

Поковба О.Ю.

Науковий керівник: **Курдеча В.В.**

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна*

E-mail: pokovba.alexander@lll.kpi.ua

Зі стрімким зростанням парадигми Інтернету речей (IoT) з'являється необхідність вибору технології, яка допоможе забезпечити високопродуктивний бездротовий зв'язок між пристроями на великих відстанях. Робота присвячена аналізу та порівнянню цих технологій передачі даних на великі відстані. Здійснено висунення та оцінку критеріїв порівняння, що включають енергоефективність, надійність, безпеку, масштабованість, пропускну здатність та інші фактори. Проаналізовано потенційні застосування в різних сферах інфокомунікацій. На основі проведеного аналізу висунуто рекомендації щодо вибору технології для конкретних застосувань.

WIRELESS TECHNOLOGIES FOR LONG-DISTANCE DATA TRANSMISSION IN IOT NETWORKS

Pokovba O.Y.

Scientific adviser: **Kurdecha V.V.**

*Educational and Scientific Institute of Telecommunication
Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine*

E-mail: pokovba.alexander@lll.kpi.ua

With the rapid growth of the Internet of Things (IoT) paradigm, there is a need to choose a technology that will help ensure high-performance wireless communication between devices over long distances. This work analyzes and compares these technologies for long-distance data transmission. The comparison criteria, including energy efficiency, reliability, security, scalability, bandwidth, and other factors, are proposed and evaluated. Potential applications in various fields of infocommunications are analyzed. Based on the analysis, recommendations are made for choosing a technology for specific applications.

ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ ВІЯВЛЕННЯ НАДЗВИЧАЙНИХ СИТУАЦІЙ

Юсин І. С.

Керівник: Курдеча В.В.

Навчально-науковий інститут телекомунікаційних

систем КПІ ім. Ігоря Сікорського, Україна

E-mail: ivanyusins@gmail.com

Задача виявлення надзвичайних ситуацій є виключно важливою для врятування людських життів, збереження матеріальних цінностей та природничого фонду. В роботі виконано дослідження можливості застосування технології Інтернету речей для виявлення та запобігання надзвичайних ситуацій. Розроблено рішення у вигляді системи реагування на надзвичайні ситуації на основі Інтернету речей та проаналізовано його ефективність та актуальність.

THE UTILIZATION OF INTERNET OF THINGS TECHNOLOGIES FOR THE DETECTION OF EMERGENCIES.

Yusyn I.S.

Scientific adviser: Kurdecha V.V.

Educational and Scientific Institute of Telecommunication

Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: ivanyusins@gmail.com

The task of detecting emergencies is crucial for saving human lives, preserving material assets, and saving the natural fund. A study has been conducted on the feasibility of employing Internet of Things technology for the detection and prevention of emergencies. A solution in the form of an emergency response system has been developed and its effectiveness and relevance have been analyzed.

МОДИФІКОВАНИЙ МЕТОД ЗАХИСТУ КІНЦЕВИХ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ

Чудо А.Р.

Науковий керівник: **Курдеча В.В.**

Навчально-науковий інститут телекомунікаційних

систем КПІ ім. Ігоря Сікорського, Україна

E-mail: chudo364@gmail.com

Стрімке зростання кількості пристроїв Інтернету речей актуалізує проблему захисту в мережі IoT. В роботі проаналізовано існуючі підходи до захисту кінцевих пристроїв IoT, виявлення їх переваг та недоліків. Модифіковано метод захисту кінцевих пристроїв Інтернету речей, що відрізняється механізмом захисту даних, та дозволяє підвищити безпеку мережі Інтернету речей. Запропоноване рішення може бути впроваджене власниками прикінцевих пристроїв мережі Інтернету речей для підвищення безпеки мережі.

A MODIFIED METHOD OF PROTECTING IOT ENDPOINTS

Chudo A.R.

Scientific adviser: **Kurdecha V.V.**

Educational and Scientific Institute of Telecommunication

Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: chudo364@gmail.com

The rapid growth in the number of Internet of Things devices makes the problem of protection in the IoT network more urgent. The paper analyzes existing approaches to protecting IoT endpoints, identifying their advantages and disadvantages. A method of protecting IoT endpoints is modified, which differs in the data protection mechanism and allows to increase the security of the IoT network. The proposed solution can be implemented by the owners of IoT endpoints to improve network security.

ОСОБЛИВОСТІ УПРАВЛІННЯ ПРИСТРОЯМИ ІНДУСТРІАЛЬНОГО ІНТЕРНЕТУ РЕЧЕЙ

Колосовський Д.О.

Науковий керівник: **Курдеча В.В.**

Навчально-науковий інститут телекомунікаційних

систем КПІ ім. Ігоря Сікорського, Україна

E-mail: kolosovskyidanyil9@gmail.com

Зростання кількості пристроїв Інтернету речей призведе до потреби у оптимізації керування мережею. Досліджено особливості управління пристроями індустриального Інтернету речей. За основу метода взята ідея децентралізації системи індустриального Інтернету речей. Запропоновано метод делегування частини управлінських рішень з основного центру прийняття рішень на кінцеві пристрої. Також задля підвищення ефективності роботи мережі пристроїв індустриального Інтернету речей запропоновано застосувати систему розподілених реєстрів до кінцевих пристроїв.

FEATURES OF INDUSTRIAL INTERNET OF THINGS DEVICE MANAGEMENT

Kolosovskyi D.O.

Scientific adviser: **Kurdecha V.V.**

Educational and Scientific Institute of Telecommunication

Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: kolosovskyidanyil9@gmail.com

The growing number of Internet of Things devices will lead to the need to optimize network management. Peculiarities of industrial Internet of Things device management were studied. The method is based on the idea of decentralization of the industrial Internet of Things system. A method of delegating a part of management decisions from the main decision-making center to end devices is proposed. Also, in order to increase the efficiency of the network of Industrial Internet of Things devices, it is proposed to apply a system of distributed registers to end devices.

ПРИНЦИП ПОБУДОВИ GPON ТА СУМІЖНИХ ГРУП ОПТОВОЛОКОННИХ ТЕХНОЛОГІЙ

Закревський М.М.

Науковий керівник: **Курдеча В.**

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна*

E-mail: maksymzakrevskiy@gmail.com

Досліджено принципи роботи технології GPON: від передачі даних до кінцевого користувача. Проаналізовано аналіз архітектури та основних компонентів GPON системи. Викладена методика розбудови міста Вишневе технологією GPON, на прикладі провайдера «БЕСТ». Розглянуті тенденції та перспективи розвитку GPON технологій у майбутньому. Зроблені висновки щодо ролі GPON у підвищенні доступності та якості телекомунікаційних послуг для користувачів. Пояснені деякі аспекти безпеки та захисту даних у контексті використання GPON технологій.

THE PRINCIPLE OF CONSTRUCTION OF GPON AND RELATED GROUPS OF OPTICAL FIBER TECHNOLOGIES

Zakrevskyy M.M.

Scientific adviser: **Kurdecha V.V.**

*Educational and Scientific Institute of Telecommunication
Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine*

E-mail: maksymzakrevskiy@gmail.com

The working principles of GPON technology are studied: from data transmission to the end user. The analysis of the architecture and main components of the GPON system was analyzed. The method of development of the city of Vyshneve using GPON technology is described, using the example of the provider "BEST". The trends and prospects for the development of GPON technologies in the future are considered. Conclusions are made regarding the role of GPON in increasing the availability and quality of telecommunication services for users. Some aspects of security and data protection in the context of using GPON technologies are explained.

ІННОВАЦІЇ ШТУЧНОГО ІНТЕЛЕКТУ В ТЕЛЕКОМУНІКАЦІЙНІЙ ІНДУСТРІЇ

Терещенко В.В.

Науковий керівник: **Курдеча В.В.**

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна
E-mail: tereshchenko.viktoria@lll.kpi.ua*

В роботі проведено огляд поточного стану штучного інтелекту (ШІ) у телекомунікаційній індустрії, його основних застосунків та потенціалу для майбутнього. Проаналізовано ключові виклики включаючи проблеми приватності, безпеки, та етичні дилеми ШІ. Виявлена здатність ШІ сприяти покращенню управління мережею, прогнозуванню вантажопотоків та оптимізації розподілу ресурсів. В рамках рішення розглянуто використання чат-ботів, віртуальних асистентів, та аналітики на основі ШІ для покращення досвіду користувачів.

ARTIFICIAL INTELLIGENCE INNOVATIONS IN THE TELECOM INDUSTRY

Tereshchenko V.V.

Scientific adviser: **Kurdecha V.V.**

*Educational and Scientific Institute of Telecommunication
Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: tereshchenko.viktoria@lll.kpi.ua*

This study conducts a comprehensive overview of the current status of artificial intelligence (AI) within the telecommunications sector, highlighting its principal applications and future potential. It delves into the critical challenges faced, including privacy concerns, security risks, and the ethical quandaries associated with AI. The research identifies AI's potential to significantly improve network management, forecast cargo flows, and optimise the allocation of resources. The paper also explores the deployment of chatbots, virtual assistants, and AI-driven analytics as means to enhance the customer experience.

ТЕНДЕНЦІ РОЗВИТКУ СТІЛЬНИКОВОГО ЗВ'ЯЗКУ

Шишкіна С.О., Коба А.О., Книр Г.А.

Науковий керівник: **Курдеча В.В.**

Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: sophia.shyshkina676@gmail.com

Розвиток стільникового зв'язку в сучасному світі набуває все більшої актуальності з ростом технологій та користувачів мобільних пристроїв. Кількість абонентів щорічно зростає мільйонами, вказуючи на стійкий попит на мобільний доступ. Зростання популярності смартфонів та планшетів стимулює пошук нових технологій для покращення якості та доступності зв'язку. Розвиток стандартів, таких як 5G, відкриває нові можливості для інновацій у сфері мобільних комунікацій, включаючи IoT. Вивчення та розробка нових технологій стільникового зв'язку має велике значення для покращення якості послуг, розвитку IoT і подальшого зростання інформаційних технологій.

TRENDS IN THE DEVELOPMENT OF CELLULAR COMMUNICATION

Shyshkina Sophia, Koba Artem, Knir Gleb

Academic Supervisor: **Kurdecha V.V.**

Educational and Scientific Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: sophia.shyshkina676@gmail.com

The development of cellular communication in the modern world is gaining increasing relevance with the growth of technologies and mobile device users. The number of subscribers increases annually by millions, indicating a steady demand for mobile access. The rising popularity of smartphones and tablets stimulates the search for new technologies to improve the quality and availability of communication. The development of standards such as 5G opens up new opportunities for innovation in mobile communications, including IoT. Studying and developing new cellular communication technologies is of great significance for improving service quality, advancing IoT, and furthering the growth of information technologies.

ПІДВИЩЕННЯ БЕЗПЕКИ В ІОТ ЗА ДОПОМОГОЮ МЕТОДІВ МАШИННОГО НАВЧАННЯ

Кузнецов Я.В.

Науковий керівник: **Курдеча В.В.**

Навчально-науковий інститут телекомунікаційних

систем КПІ ім. Ігоря Сікорського, Україна

E-mail: kuznetsov.yaroslav@lil.kpi.ua

ІоТ (інтернет речей) забезпечує сполучення різноманітних пристроїв для надання розумних послуг, але вимагає надійного захисту від кібер загроз. Методи машинного навчання (МН) відкривають нові можливості для підвищення безпеки в ІоТ. Досліджено моделі атак для ІоТ та розглянуто заходи захисту, використовуючи методи МН. Аутентифікація, контроль доступу та виявлення шкідливих програм – основні напрямки застосування МН для захисту в ІоТ. Виклики, пов'язані з впровадженням методів МН для забезпечення безпеки в практичних системах інтернету речей.

ENHANCING IOT SECURITY USING MACHINE LEARNING TECHNIQUES

Kuznetsov Y.V.

Scientific adviser: **Kurdecha V.V.**

Educational and Scientific Institute of Telecommunication

Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: kuznetsov.yaroslav@lil.kpi.ua

IoT (Internet of Things) facilitates the connection of various devices to provide smart services but requires robust protection against cyber threats. Machine learning (ML) methods open up new opportunities for enhancing security in IoT. Attack models for IoT have been investigated, and security measures using ML methods have been discussed. Authentication, access control and malware detection are the primary areas of ML application for IoT security. Challenges regarding the implementation of ML-based security schemes into practical IoT systems.

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ В СФЕРІ КОМЕРЦІЙНОЇ ТОРГІВЛІ

Журба І.О.

Науковий керівник: **Курдеча В.В.**

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна*

E-mail: izhurba321@gmail.com

Актуальність застосування IoT в сфері комерційної торгівлі полягає у можливості покращення ефективності бізнесу та підвищенні конкурентоспроможності, спрощуючи процеси для персоналу та забезпечуючи зручність для покупців. В роботі запропонована модифікація методу управління обігом товару за рахунок автоматизації процесів на основі технології Інтернету речей.

FEATURES OF THE APPLICATION OF THE INTERNET OF THINGS TECHNOLOGIES IN THE FIELD OF COMMERCIAL TRADE

Zhurba I. O.

Scientific adviser: **Kurdecha V.V.**

*Educational and Scientific Institute of Telecommunication
Systems Igor Sikorsky Kyiv Polytechnic Institute, Ukraine*

E-mail: izhurba321@gmail.com

The relevance of IoT application in the field of commercial trade lies in the possibility of improving business efficiency and increasing competitiveness, simplifying processes for staff and providing convenience for buyers. The article proposes a modification of the method of managing the circulation of goods due to the automation of processes based on the Internet of Things technology.

РОЗВИТОК ТА ІНТЕГРАЦІЯ ТЕХНОЛОГІЙ 6G ДЛЯ МАЙБУТНЬОГО ПОКОЛІННЯ МОБІЛЬНОГО ЗВ'ЯЗКУ

Голуб А.С.

Науковий керівник: **Курдеча В.В.**

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна*

E-mail: holub.anna@lil.kpi.ua

Дослідження спрямоване на визначення ключових аспектів технологічного розвитку та впровадження новаторських рішень у сфері бездротового зв'язку. Основною метою є вивчення та аналіз майбутнього покоління мобільних комунікаційних технологій - 6G. У цій роботі розглядаються очікування щодо 6G технологій і розвитку майбутніх мобільних зв'язків, враховуючи високі вимоги до швидкості та надійності в комунікаціях нового покоління.

DEVELOPMENT AND INTEGRATION OF 6G TECHNOLOGIES FOR THE FUTURE GENERATION OF MOBILE COMMUNICATION

Holub A.S.

Scientific adviser: **Kurdecha V.V.**

*Educational and Scientific Institute of Telecommunication
Systems Igor Sikorsky Kyiv Polytechnic Institute, Ukraine*

E-mail: holub.anna@lil.kpi.ua

The research is aimed at determining the key aspects of technological development and implementation of innovative solutions in the field of wireless communication. The main goal is to study and analyze the future generation of mobile communication technologies - 6G. This work examines the expectations for 6G technologies and the development of future mobile communications, taking into account the high requirements for speed and reliability in new generation communications.

МОЖЛИВОСТІ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ LI-FI В МЕРЕЖІ INTERNET OF THINGS

Руденко А.А.

Науковий керівник: **Курдеча В.В.**

*Навчально-науковий інститут телекомунікаційних
систем, КПІ ім. Ігоря Сікорського, Україна*

E-mail: ana

stasiarudenko078@gmail.com

Інтернет речей стрімко розвивається і в найближчому майбутньому, коли пристрої масово поширяться, може постати проблема в якій мережа Wi-Fi може бути перенасичена трафіком між IoT пристроями. Тому необхідно дослідити нові способи передачі даних, у тому числі і за допомогою Li-Fi. В публікації досліджено використання технології Li-Fi в мережі Інтернету речей. Особливу увагу приділено можливості та проблеми організації мережі, яка працювала у спектрі видимого світла та інфрачервоного спектру.

THE USAGE OF LI-FI TECHNOLOGY IN THE INTERNET OF THINGS NETWORK

Rudenko A.A.

Scientific adviser: **Kurdecha V.V.**

*Educational and Scientific Institute of Telecommunication
Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine*

E-mail: anastasiarudenko078@gmail.com

The Internet of Things is developing rapidly, and in the near future, when the devices become widespread, a problem may arise in which the Wi-Fi network may be oversaturated with traffic between IoT devices. Therefore, it is necessary to investigate new methods of data transmission, including with the help of Li-Fi. The publication examines the use of Li-Fi technology in the Internet of Things network. Special attention was paid to the possibilities and problems of organizing a network that worked in the spectrum of visible light and the infrared spectrum.

МОДИФІКОВАНА МОДЕЛЬ КОРПОРАТИВНОЇ МЕРЕЖІ ЗВ'ЯЗКУ

Нечипоренко А.С.

Науковий керівник: **Курдеча В.В.**

*Навчально-науковий інститут телекомунікаційних
систем, КПІ ім. Ігоря Сікорського, Україна*

E-mail: rtmneciporenko@gmail.com

Проаналізовано корпоративні мережі зв'язку та їх процес розробки на базі існуючих моделей корпоративних мереж й модифіковано її модель в частині безпроводової передачі даних з використанням технології Wi-Fi 6. Сформовано рекомендації по розробці корпоративної мережі зв'язку на основі модифікованої моделі. Проведено натурне моделювання запропонованого рішення з використанням спеціалізованого ПО (Cisco Pocket Tracer).

MODIFIED MODEL OF CORPORATE COMMUNICATION NETWORK

Nechyporenko A.S.

Scientific adviser: **Kurdecha V.V.**

*Educational and Scientific Institute of Telecommunication
Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine*

E-mail: rtmneciporenko@gmail.com

The analysis of corporate communication networks and their developmental procedures was undertaken based on existing models of corporate networks. Subsequently, the model of corporate communication networks was adapted with a focus on wireless data transmission, incorporating Wi-Fi 6 technology. Recommendations for the development of corporate communication networks were then formulated, drawing from the modified model. Finally, natural modeling of the proposed solution was executed utilizing specialized software, specifically Cisco Packet Tracer.

СУПРОВОДЖЕННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ БАНКІВСЬКОЇ УСТАНОВИ

Посвистьол В.В.

Науковий керівник: **Курдеча В.В.**

*Навчально-науковий інститут телекомунікаційних систем, КПІ ім. Ігоря Сікорського, Україна
E-mail: vladislav.posvistol@gmail.com*

В роботі виявлено необхідність вдосконалення супроводження інформаційних систем у банківських установах для забезпечення їхньої ефективності. Метою був аналіз сучасних методів та практики супроводження інформаційних систем та виявлення можливостей для покращення. На основі дослідження було виявлено, що частка банківських установ мають проблеми з ефективним супроводженням інформаційних систем, що може призвести до загроз для їхньої безпеки та функціонування. Результат показує необхідність подальшого вдосконалення практик супроводження інформаційних систем у банківській сфері для забезпечення надійності та стабільності в них.

SUPPORT OF THE INFORMATION SYSTEM OF A BANKING INSTITUTION

Posvystol V.V.

Scientific adviser: **Kurdecha V.V.**

*Educational and Scientific Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: vladislav.posvistol@gmail.com*

The study identified the need to improve the maintenance of information systems in banking institutions to ensure their effectiveness. The aim was to analyze current methods and practices of information systems maintenance and identify opportunities for improvement. The study revealed that a share of banking institutions have problems with effective support of information systems, which can lead to threats to their security and functioning. Result shows the need for further improvement of information systems support practices in the banking sector to ensure reliability and stability in them.

ОПТИМІЗАЦІЯ ЕНЕРГОПОСТАЧАННЯ ТА СПОЖИВАННЯ ЧЕРЕЗ СТАТИСТИЧНИЙ АНАЛІЗ ДАНИХ

Корнійчук І.Г.

Науковий керівник: **Курдеча В.В.**

*Навчально-науковий Інститут телекомунікаційних
систем, КПІ ім. Ігоря Сікорського, Україна*

E-mail: korniichuk2002@gmail.com

Статистичний аналіз даних для оптимізації енергопостачання та енергоспоживання стає все більш актуальним у сучасному світі, де енергетична ефективність та стійкість відіграють ключову роль. Однак, варіабельність та непередбачуваність споживання енергії можуть створювати виклики для стабільного та ефективного енергопостачання. У роботі досліджено, як статистичний аналіз даних може допомогти в управлінні енергопостачанням, зменшенні експлуатаційних витрат та підвищенні енергоефективності.

OPTIMIZATION OF ENERGY SUPPLY AND CONSUMPTION THROUGH STATISTICAL DATA ANALYSIS

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

Statistical data analysis to optimize energy supply and consumption is becoming increasingly relevant in today's world, where energy efficiency and sustainability play a key role. However, the variability and unpredictability of energy consumption can pose challenges to a stable and efficient energy supply. This paper explores how statistical data analysis can help manage energy supply, reduce operating costs, and improve energy efficiency.

ОЦІНКА СУМІСНОСТІ СЛОТОВИХ ФОРМАТІВ СИГНАЛУ В МЕРЕЖАХ 5G

Тичинський - Мартинюк В.Ю.

Науковий керівник: **Якорнов Є.А.**

*Навчально-науковий інститут телекомунікаційних
систем, КПІ ім. Ігоря Сікорського, Україна
E-mail: tychynskiy-martyniuk.vitalii@lil.kpi.ua*

Одним із удосконалень на рівні управління радіоресурсом в стандарті 5G NR є гнучка конструкція, заснована на концепції часових слотів (інтервалів). Комбінації форматів слотів із гнучкими символами дозволяють ефективно використовувати мережеві ресурси, а також забезпечувати сумісність обладнання під час спільного використання частотного ресурсу або використання суміжних частотних каналів. У доповіді наводяться результати оцінки сумісності варіацій групи форматів слотів з метою їх використання базовими станціями 5G NR в різних умовах радіозавад і підтримки трафіку.

COMPATIBILITY ASSESSMENT OF SIGNAL SLOT FORMATS IN 5G NETWORKS

Tychynskiy - Martyniuk V.Yu.

Scientific supervisor: **Yakornov E.A.**

*Educational and Scientific Institute of Telecommunication
Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: tychynskiy-martyniuk.vitalii@lil.kpi.ua*

One of enhancements at the level of radio resource management in 5G NR standard is a flexible design based on time slots conception. Combinations of slot formats with flexible symbols allows the efficient use of network resources as well as ensuring equipment compatibility when sharing frequency resource or using adjacent frequency channels. The report provides results of assessment the compatibility of the slot formats group variations for the purpose of their usage by 5G NR base stations in various interference conditions and traffic support.

УДОСКОНАЛЕННЯ ІНФОКОМУНІКАЦІЙНОГО АУДИТУ

Ковальська Д.Д.

Науковий керівник: **Якорнов Є.А.**

Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: zashkvar.youtuba01@gmail.com

Досліджено особливості та слабкі місця проведення інфокомунікаційного аудиту з допомогою натурального експерименту. Однією з головних проблем аудиту великих мереж є необхідність всебічного аналізу всієї інфраструктури для виявлення потенційних проблем, ризиків і слабких місць. Модифікація стандартних методів аудиту шляхом використання програмного забезпечення є перспективним та ефективним підходом, оскільки дозволяє забезпечити високий рівень точності та виключення ризиків людської помилки.

IMPROVEMENT OF INFOCOMMUNICATION AUDIT

Kovalaska D.D.

Scientific adviser: **Yakornov Y.A.**

Educational and Scientific Institute of Telecommunication Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: zashkvar.youtuba01@gmail.com

The specific features and weak points of the information communication audit were studied with the help of a natural experiment. One of the main challenges of auditing large networks is the need to comprehensively analyze the entire infrastructure to identify potential problems, risks and weaknesses. Modification of standard audit methods through the use of software is a promising and effective approach, as it allows to ensure a high level of accuracy and eliminate the risks of human error.

АНАЛІЗ СИСТЕМ РОЗУМНОГО БУДИНКУ ДЛЯ ЛЮДЕЙ З ОБМЕЖЕНИМИ МОЖЛИВОСТЯМИ

Оленюк М.М.

Науковий керівник: **Курдеча В.В.**

Навчально-науковий Інститут телекомунікаційних систем, КПІ ім. Ігоря Сікорського, Україна

E-mail: kolyaolenyuk1234@gmail.com

Світ стрімко розвивається, і технології роблять наше життя все більш комфортним. Для людей з обмеженими можливостями це особливо актуально, адже розумні будинки дарують їм шанс на більш самостійне та повноцінне життя. Розумні будинки – це не просто модний тренд, а реальний шанс на покращення життя людей з обмеженими можливостями. Завдяки доступним технологіям вони можуть жити більш самостійно, безпечно та комфортно.

У цій роботі досліджується, як підвищити функціональність систем розумного будинку у контексті питань безпеки та охорони здоров'я шляхом застосування рішень інтернету-речей.

ANALYSIS OF SMART HOME SYSTEMS FOR PEOPLE WITH DISABILITIES

Olenyuk M.M.

Scientific adviser: **Kurdecha V.V.**

*Educational and Scientific Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine*

E-mail: kolyaolenyuk1234@gmail.com

The world is developing rapidly, and technology is making our lives more and more comfortable. This is especially relevant for people with disabilities, because smart houses give them a chance for a more independent and fulfilling life. Smart homes are not just a fashion trend, but a real chance to improve the lives of people with disabilities. Thanks to available technology, they can live more independently, safely and comfortably.

This work investigates how to increase the functionality of smart home systems in the context of safety and health issues by applying Internet of Things solutions.

ЗАСТОСУВАННЯ ІТ ІНСТРУМЕНТІВ У ПОШУКУ МОНЕТ

Гінзбург А.І., Ігнатова С.С.

Науковий керівник: **Комаров І.Ю.**

Політехнічний ліцей КПІ ім. Ігоря Сікорського,

Комунальний заклад позашкільної освіти

«Київська Мала академія наук учнівської молоді», Україна

E-mail: plkpi_kvnt@ukr.net

В роботі описано створення програми, яка спрощує пошук монет Римської імперії. Додаток працює за принципом пошуку співпадінь у базі даних. Користувач може вводити легенду монети або її частину, а програма шукатиме співпадиння в базі даних і виводить можливі варіанти монет. Додаток є корисним для нумізматів різного рівня досвіду. Він простий у використанні для початківців, але також містить функції, які будуть цікавими для досвідчених нумізматів. Також він може бути цікавим для науковців, які вивчають історію Римської імперії.

Ключові слова: БАЗА ДАНИХ, РИМСЬКА ІМПЕРІЯ, МОНЕТИ, PYTHON, DJANGO ORM, НУМІЗМАТИКА.

APPLICATION OF IT TOOLS IN THE SEARCH OF COINS

The work describes the creation of a program that simplifies the search for coins of the Roman Empire. The application works on the principle of searching for matches in the database. The user can enter the legend of the coin or part of it, and the program will search for a match in the database and display possible coin variants. The application is useful for numismatists of all levels of experience. It is easy to use for beginners, but also contains features that will be of interest to experienced numismatists. It may also be of interest to scholars studying the history of the Roman Empire.

СТВОРЕННЯ ТА ЗАСТОСУВАННЯ ТЕЛЕГРАМ БОТУ “RECOMMENDIFY”

Обозовий І.Ю., Ігнатова С.С.

Науковий керівник: **Комаров І.Ю.**

Політехнічний ліцей КПІ ім. Ігоря Сікорського,

Комунальний заклад позашкільної освіти

«Київська Мала академія наук учнівської молоді», Україна

E-mail: plkpi_kvnt@ukr.net

В роботі досліджено створення та застосування алгоритмів стрімінгових сервісів, їхні плюси та мінуси. Створено бот в допомогу людям, які хочуть відійти від Spotify, що підбирає ідеально персоналізовану музику за аналогією попередніх прослуховувань. Телеграм бот Reecommendify допоможе знайти альбоми будь-яких жанрів, будь-яких настроїв, будь-яких текстів, форм, тонів або стилів.

Ключові слова: ТЕЛЕГРАМ БОТ, PYTHON, МУЗИКА, SPOTIFY, АЛЬБОМ, ЖАНР, ОПИС, ДАТАБАЗА, КОД.

CREATION AND APPLICATION OF TELEGRAM BOT “RECOMMENDIFY”

The work explores the creation and application of streaming service algorithms, their pros and cons. A bot has been created to help people who want to leave Spotify, which selects perfectly personalized music based on previous listening. Telegram bot Reecommendify will help you find albums of any genre, any mood, any lyrics, shapes, tones or styles.

Key words: TELEGRAM BOT, PYTHON, MUSIC, SPOTIFY, ALBUM, GENRE, DESCRIPTOR, DATABASE, CODE.

РОЗВИТОК ПРОГРАМНО-АПАРАТНИХ ЗАСОБІВ ВИМІРЮВАННЯ В УКРАЇНІ (ДРУГА ПОЛОВИНА ХХ СТ.)

Хіхло В.Ю.

Науковий керівник: **Тверитникова О.Є.**

Національний технічний університет

«Харківський політехнічний інститут», Україна

E-mail: vadym.khikhlo@sgt.khpi.edu.ua

Встановлено та досліджено основні етапи створення інформаційно-вимірювальних систем, а також окреслено внесок українських вчених Національної академії наук України, зокрема Інституту електродинаміки, Інституту кібернетики, політехнічних закладів вищої освіти у створення вимірювального устаткування нового покоління упродовж 1950–1990-х рр. Показано, що ускладнення технологій виробництва та розвиток наукових досліджень зумовили появу нового класу інформаційно-вимірювальної техніки, здатної здійснювати збір, обробку, передачу, зберігання та відображення інформації щодо об'єктів дослідження, зокрема віртуальних та інтелектуальних вимірювальних приладів і систем.

EVOLUTION OF SOFTWARE AND HARDWARE MEASURING TOOLS IN UKRAINE (SECOND HALF OF THE TWENTIETH CENTURY)

Khikhlo V.Y.

Scientific adviser: **Tverytnykova O.Y.**

National Technical University "Kharkiv Polytechnic Institute", Ukraine

E-mail: vadym.khikhlo@sgt.khpi.edu.ua

The main stages of developing information and measurement systems are identified and studied. Also, the contribution of Ukrainian scientists of the National Academy of Sciences of Ukraine, particularly the Institute of Electrodynamics, the Institute of Cybernetics, and polytechnic higher education institutions, to creating new generation measuring equipment in the 1950s–1990s is outlined. It is shown that the complication of production technologies and the progress of scientific research have led to the emergence of a new class of information and measuring equipment capable of collecting, processing, transmitting, storing, and displaying information about research objects, including virtual and intelligent measuring devices and systems.

**РОЗРОБКА АЛГОРИТМУ АВТОКОМПЕНСАЦІЇ
САМОІНТЕРФЕРЕНЦІЙНИХ СИГНАЛІВ В
АНТЕНОХВИЛЕВОДНОМУ ТРАКТІ КАНАЛУ ПРИЙОМУ ДЛЯ
ОДНОЧАСТОТНИХ СИСТЕМ РАДІОРЕЛЕЙНОГО ЗВ'ЯЗКУ**

Омельченко С.А.

Науковий керівник: **Якорнов Є.А.**

Навчально-науковий інститут телекомунікаційних

систем КПІ ім. Ігоря Сікорського, Україна

E-mail: omelchenko.svitlana@lil.kpi.ua

У доповіді пропонується алгоритм компенсації самоінтерференційних сигналів у радіорелейних системах зв'язку. На основі аналізу природи завад наведені перші кроки розробки алгоритму компенсації. Вказано на переваги цього алгоритму, його обмеження та підкреслено важливість цієї розробки для покращення радіорелейних систем зв'язку.

**DEVELOPMENT OF AN ALGORITHM FOR AUTO-COMPENSATION
OF SELF-INTERFERENCE SIGNALS IN THE ANTENNA-WAVEGUIDE
PATH OF THE RECEIVING CHANNEL FOR SINGLE-FREQUENCY
RADIO RELAY COMMUNICATION SYSTEMS**

Omelchenko S.A.

Scientific adviser: **Yakornov Y. A.**

Educational and Scientific Institute of Telecommunication

Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

E-mail: omelchenko.svitlana@lil.kpi.ua

The paper proposes an algorithm for compensating for self-interference signals in radio relay communication systems. Based on the analysis of the nature of interference, the first steps in the development of the compensation algorithm are presented. The advantages of this algorithm, its limitations, and the importance of this development for the improvement of radio relay communication systems are emphasized.

ДОСЛІДЖЕННЯ МЕТОДІВ ІНТЕЛЕКТУАЛЬНОЇ МАРШРУТИЗАЦІЇ В ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖАХ

Майба М.А.

Науковий керівник: **Єременко О.С.**

Харківський національний університет радіоелектроніки, Україна

E-mail: mykola.maiba@nure.ua

Досліджено використання методів інтелектуальної маршрутизації в програмно-конфігурованих мережах. Обґрунтовано важливість використання штучного інтелекту в системах управління трафіком для забезпечення якості обслуговування в мережах. Виконано порівняння різних моделей машинного навчання, включаючи лінійну регресію, логістичну регресію, дерева рішень і випадковий ліс. Розроблено програмний модуль, який використовує прогнозовані дані навченої моделі для розв'язання задачі оптимізації. Розглянуто використання різнотипних метрик для визначення оптимального маршруту в мережі, а саме метрики по аналогії з протоколами RIP, OSPF та на основі ймовірності компрометації для визначення оптимального маршруту.

RESEARCH OF INTELLIGENT ROUTING METHODS IN SOFTWARE-DEFINED NETWORKS

Maiba M.A.

Scientific adviser: **Yeremenko O.S.**

Kharkiv National University of Radio Electronics, Ukraine

E-mail: mykola.maiba@nure.ua

The use of intelligent routing methods in software-defined networks is investigated. The importance of using artificial intelligence in traffic management systems to ensure the Quality of Service in networks is substantiated. Various machine learning models are compared, including linear regression, logistic regression, decision trees, and random forest. A software module is developed that uses the predicted data of the trained model to solve the optimization problem. The use of various metrics for determining the optimal route in the network is considered, namely metrics by analogy with RIP, OSPF protocols and based on the compromise probability to determine the optimal route.

АНАЛІЗ ШЛЯХІВ ЕФЕКТИВНОГО ЗАХИСТУ СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ ВІД КІБЕРЗАГРОЗ

Іванова Т.С.

Науковий керівник: **Уривський Л.О.**

*Навчально-науковий інститут телекомунікаційних
систем, КПІ ім. Ігоря Сікорського, Україна*

E-mail: ivanovatwork31@gmail.com

Розглянуто процеси створення та інтеграції програмного забезпечення для підвищення рівня безпеки підключених пристроїв Інтернету речей (IoT). Через стрімкий розвиток IoT та зростання кількості підключених пристроїв, забезпечення їхньої безпеки стає надзвичайно важливим завданням. Доповідь охоплює аналіз потенційних загроз, дослідження сигнатур для виявлення шкідливого програмного забезпечення, можливості інтеграції з існуючими протоколами IoT, а також процес впровадження та підтримки антивірусного ПЗ. Детальний аналіз загроз та стратегічний підхід до розробки та впровадження гарантують ефективний захист підключених пристроїв IoT від широкого спектру кіберзагроз.

THE WAYS OF IoT SYSTEMS EFFECTIVE PROTECTION FROM CYBER THREATS

Ivanova T.

Scientific adviser: **Uryvsky L.**

*Educational and Scientific Institute of Telecommunication
Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine*

E-mail: ivanovatwork31@gmail.com

The processes of creating and integrating software to improve the security of connected Internet of Things (IoT) devices are considered. Due to the rapid development of the IoT and the growing number of connected devices, ensuring their security is becoming an extremely important task. The report covers the process of analyzing potential threats, researching signatures to detect malware, integrating with existing IoT protocols, and the process of implementing and maintaining antivirus software. Detailed threat analysis and a strategic approach to design and implementation ensure that connected IoT devices are effectively protected from a wide range of cyber threats.

МАШИННЕ НАВЧАННЯ У АВТОМАТИЗАЦІЇ РОБОТИ ДАТАЦЕНТРУ

Кравченко І.М.

Науковий керівник: **Міночкін Д.А.**

*Навчально-науковий інститут телекомунікаційних
систем, КПІ ім. Ігоря Сікорського, Україна*

E-mail: il.kravchenko115@gmail.com

Досліджено можливості та переваги автоматизації роботи датацентру з використанням машинного навчання. Проаналізовано способи та приклади застосування машинного навчання для автоматизації роботи датацентрів. Застосування машинного навчання для розробки автоматизації протипожежної системи датацентрів, як один із способів автоматизованої роботи датацентру.

MACHINE LEARNING IN DATA CENTER AUTOMATION

Kravchenko I.M.

Scientific adviser: **Minochkin D.A.**

*Educational and Scientific Institute of Telecommunication
Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine*

E-mail: il.kravchenko115@gmail.com

The possibilities and advantages of automating data centre operations using machine learning are investigated. The ways and examples of machine learning application for data centre automation are analysed. Application of machine learning for the development of automation of the data centre fire protection system as one of the ways to automate the data centre.

МЕТОДИ СТИСКУ ДАНИХ В БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ

Третяк А.В.

Науковий керівник: **Лисенко О.І.**

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна*

E-mail: petbka.tasher@gmail.com

В роботі проаналізовано різні методи стиснення даних, що використовуються в бездротових сенсорних мережах. Розглядаються чотири основні категорії: стиснення на основі рядків, на основі зображень, кодування розподіленого джерела та стиснуте зондування. Порівняння цих методів за можливістю відновлення даних, без втрат або з втратами. Наводяться алгоритми в кожній категорії, пояснюється їх принцип дії.

METHODS OF DATA COMPRESSION IN WIRELESS SENSOR NETWORKS

Tretiak A.V.

Scientific adviser: **Lysenko O.I.**

*Educational and Scientific Institute of Telecommunication
Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine*

E-mail: petbka.tasher@gmail.com

The article analyzes various methods of data compression used in wireless sensor networks. Four main categories are considered: string-based compression, image-based compression, distributed source coding, and compressed sensing. Comparison of these methods for data recovery, lossless or lossy. Algorithms in each category are given, and their principle of action is explained.

**РОЗРОБКА СИСТЕМИ ЦИФРОВОГО РАДІОРЕЛЕЙНОГО
ЗВ'ЯЗКУ ПІДВИЩЕНОЇ ПРОПУСКНОЇ ЗДАТНОСТІ НА
ОСНОВІ ЗАСТОСУВАННЯ СФЕРИЧНОСТІ ФРОНТУ
ЕЛЕКТРОМАГНІТНОЇ ХВИЛІ В ЗОНІ ФРЕНЕЛЯ**

Мінжинер Н.М.

Науковий керівник: **Якорнов Є.А.**

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна*

E-mail: minzinernina@gmail.com

Показано можливість застосування просторової селекції радіосигналів для підвищення пропускної здатності дуплексної одноінтервальної цифрової радіорелейної лінії зв'язку шляхом введення для її просторової обробки радіосигналів за формою фазового фронту електромагнітної хвилі та запропонована технічне рішення системи для її використання.

**DEVELOPMENT OF HIGH THROUGHPUT DIGITAL
RADIO RELAY COMMUNICATION SYSTEM BASED ON THE
APPLICATION OF SPHERICITY OF ELECTROMAGNETIC WAVE
FRONT IN THE FRESNEL ZONE**

Minzhyner N.M.

Scientific adviser: **Yakornov Y. A.**

*Educational and Scientific Institute of Telecommunication
Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine*

E-mail: minzinernina@gmail.com

The aim of this research is to theoretically prove and practically demonstrate the feasibility of applying spatial selection of radio signals to solve the problem of reusing radio frequency resources in duplex single-interval digital radio relay communication lines. This is achieved through the development of a method for spatial selection of radio signals based on the shape of the phase front of their electromagnetic waves for a digital radio relay station and the technical solution based on it.

МЕТОДИ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ТА ЦІЛІСНОСТІ ІНФОРМАЦІЇ В МЕРЕЖІ 5G МІЛІМЕТРОВОГО ДІАПАЗОНУ

Скомаха М.О.

Науковий керівник: Єременко О.С.

Харківський національний університет радіоелектроніки, Україна

E-mail: mykyta.skomakha@nure.ua

Проведено аналіз стану інформаційної безпеки та класифіковано атаки на мережу 5G шляхом побудови сценаріїв загроз та засобів протидії. Для дослідження обрано мобільну мережу 5G з високочастотним спектром. Розглянуто методи захисту від глушіння та перехоплення сигналу в технології mMIMO, застосування шифрування та протоколів захисту мережі IPsec, IKEv2 та TLS. Також розглянуто реєстрацію й автентифікацію пристроїв, використання проксі-сервера в роумінгу. На основі аналізу визначено вразливість перед впровадженням модифікованих складових загальної інфраструктури 5G у вигляді базових станцій та користувацьких пристроїв, слабкість мережі до DoS атак та недосконалість криптографічного шифрування окремих пристроїв.

METHODS FOR ENSURING THE INFORMATION CONFIDENTIALITY AND INTEGRITY IN MILLIMETRE WAVE 5G NETWORK

Skomakha M.O.

Scientific adviser: Yeremenko O.S.

Kharkiv National University of Radio Electronics, Ukraine

E-mail: mykyta.skomakha@nure.ua

An analysis of the state of information security is carried out, and attacks on the 5G network are classified by building threat scenarios and countermeasures. The 5G mobile network with a high-frequency spectrum is chosen for the study. The methods of protection against jamming and signal interception in mMIMO technology, as well as the use of encryption and network protection protocols IPsec, IKEv2, and TLS, are considered. Registration and authentication of devices and using a proxy server when roaming are also considered. Based on the analysis, the vulnerability before the introduction of modified components of the overall 5G infrastructure in the form of base stations and user devices, the network's weakness to DoS attacks, and the imperfection of cryptographic encryption of individual devices are identified.

ТЕНДЕНЦІЇ РОЗВИТКУ СИСТЕМ ДОСТУПУ BLUETOOTH ТА WI-FI

Ковальов А.В.

Науковий керівник: **Курдеча В.В.**

*Навчально-науковий інститут телекомунікаційних
систем, КПІ ім. Ігоря Сікорського, Україна*

E-mail: kovalov.andriy@lil.kpi.ua

Досліджено тенденції розвитку систем доступу Bluetooth та Wi-Fi, а саме: нові стандарти, протоколи безпеки (WPA3, Bluetooth LE Secure Connections), їх енергоспоживання, сфери застосування (Інтернет речей IOT, розумні будинки, промислова автоматизація та ін.). Окремо було проаналізовано майбутнє бездротових технологій за прогнозами компаній-гігантів та ключових спеціалістів у сфері інфокомунікацій.

TRENDS IN THE DEVELOPMENT OF ACCESS SYSTEMS BLUETOOTH AND WI-FI

Kovalev A.V.

Scientific adviser: **Kurdecha V.V.**

*Educational and Scientific Institute of Telecommunication
Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine*

E-mail: kovalov.andriy@lil.kpi.ua

The trends in the development of Bluetooth and Wi-Fi access systems are investigated, namely: new standards, security protocols (WPA3, Bluetooth LE Secure Connections), their power consumption, areas of application (Internet of Things IOT, smart homes, industrial automation, etc.). The future of wireless technologies was also analyzed according to the forecasts of giant companies and key specialists in the field of infocommunications.

ДОСЛІДЖЕННЯ ПИТАННЯ ЕФЕКТИВНОСТІ ТА ВИПРАВНОЇ ЗДАТНОСТІ КОДІВ РІДА-СОЛОМОНА

Косогор А.В.

Науковий керівник: **Уривський Л.О.**

*Навчально-науковий інститут телекомунікаційних
систем, КПІ ім. Ігоря Сікорського, Україна*

E-mail: kosogor.anastasia@lll.kpi.ua

Досліджено питання ефективності використання кодів Ріда-Соломона на прикладі QR-кодів; як їм знайшли застосування саме у цьому напрямку. Проаналізовано можливості коду виправляти різноманітні багатократні помилки: групові помилки (плями), окремі символи, послідовність повністю пошкоджених символів, послідовність частково пошкоджених символів, окремих бітів. Де саме у QR-коді зберігається інформація, на що вона розподіляється і як працює, та яким чином у деяких випадках код може виправити близько 60 пошкоджених бітів, а в яких не здатен виправити і 5 бітів.

PROCESSING CALL AND DETAIL RECORDS IN THE SOFT SWITCH FREESWITCH

Kosohor A.V.

Scientific adviser: **Uryvsky L.O.**

*Educational and Scientific Institute of Telecommunication
Systems, Igor Sikorsky Kyiv Polytechnic Institute, Ukraine*

E-mail: kyiv12@bigmir.net

The issue of the effectiveness of using Reed-Solomon codes on the example of QR codes is investigated; how they are used in this direction. Analyzed the code's ability to correct various multiple errors: group errors (spots), individual characters, a sequence of completely damaged characters, a sequence of partially damaged characters, and individual bits. Where exactly is the information stored in the QR code, what is it allocated to and how it works, and how in some cases the code can fix about 60 damaged bits, and in others it cannot fix even 5 bits.